(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－133384
（P2002－133384A）
(43)公開日　平成14年５月10日(2002.5.10)

(51)Int.Cl.[7]		識別記号	FI			テーマコード*（参考）
Ｇ０６Ｋ	19/073		Ｂ４２Ｄ	15/10	５２１	２Ｃ００５
Ｂ４２Ｄ	15/10	５２１	Ｇ０６Ｆ	15/00	３３０Ｇ	５Ｂ０３５
Ｇ０６Ｆ	1/00			17/60	２２２	５Ｂ０５５
	15/00	３３０	Ｇ０６Ｋ	19/00	Ｐ	５Ｂ０７６
	17/60	２２２	Ｇ０６Ｆ	9/06	６６０Ｅ	５Ｂ０８５

審査請求　未請求　請求項の数10　ＯＬ　（全 26 頁）

(21)出願番号　特願2000－318428(P2000－318428)

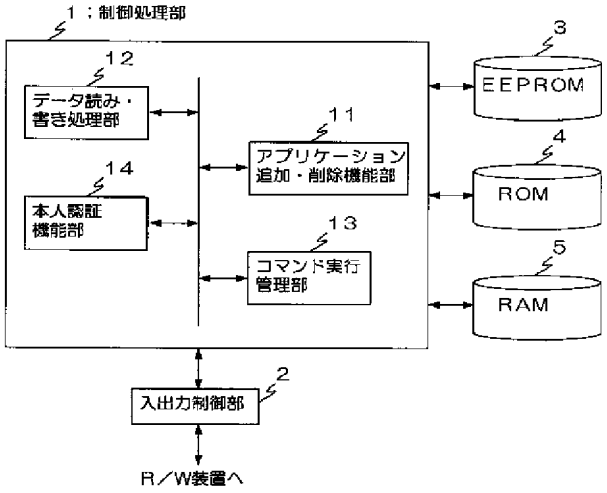
(22)出願日　平成12年10月18日(2000.10.18)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　飯野　徹
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　岩瀬　史幸
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　ＩＣカード、登録装置、及びサービス提供システム

(57)【要約】
【課題】　複数のサービスから、ＩＣカード内の本人認証機能を共有し、サービス利用者自身が複数の本人認証方法を、安全性を損なわない範囲で選択できるＩＣカード、登録装置、及びサービス提供システムを提供する。
【解決手段】　本人認証機能部１４は、ＥＥＰＲＯＭ３に記録された認証方法を用いて、ＥＥＰＲＯＭ３に記録された本人を特定する認証用テンプレートと、コマンド実行管理部１３がアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較して、アプリケーションプログラムが指定する認証方法によるＩＣカード使用者の認証を行う。ＩＣカード上で実行されるアプリケーションプログラムは、アプリケーション追加・削除機能部１１により管理され、アプリケーションプログラムが要求する認証方法や認証用テンプレート等を含む認証情報の登録はデータ読み・書き処理部１２により管理される。



【特許請求の範囲】
【請求項１】　ＩＣカード上に記録されたアプリケーションプログラムによりサービスを提供するＩＣカードであって、
前記ＩＣカードで実行される複数の前記アプリケーションプログラム、及び前記アプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録する記録手段と、
前記記録手段に記録された認証方法を用いて、前記記録手段に記録された本人を特定する認証用データと、前記記録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりＩＣカード使用者の認証を行う本人認証手段と、
前記本人認証手段において認証が行われることにより前記記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行手段と、
を設けたことを特徴とするＩＣカード。
【請求項２】　前記本人認証手段は、
前記認証方法の実行結果を予め設定された点数により取得する手段と、
予め設定された優先順位に従い実行される複数の前記認証方法の実行結果として出力された前記点数を加算する手段と、
加算された前記点数とアプリケーションプログラムの指定する所定の点数とを比較する手段と、
を更に含み、
前記アプリケーションプログラムの指定する所定の点数を満たした時点で、前記アプリケーションに認証の正常終了を通知することを特徴とする請求項１に記載のＩＣカード。
【請求項３】　前記本人認証手段は、
前記認証方法の実行結果を予め設定された点数により取得する手段と、
前記認証方法の実行結果として出力された現在の点数と次に実行するアプリケーションプログラムの指定する所定の点数とを比較する手段と、
比較の結果、前記アプリケーションプログラムの指定する所定の点数が前記現在の点数より大きい場合、前記アプリケーションプログラムに指定された認証方法を実行し、該認証方法による点数を新しい現在の点数として記録・更新する手段と、
を更に含み、
認証結果による現在の点数が、前記アプリケーションプログラムの指定する所定の点数を満たしていた場合、該アプリケーションプログラムの指定する認証方法の実行を省略することを特徴とする請求項１に記載のＩＣカード。
【請求項４】　前記本人認証手段は、
認証に使用する前記認証用データが複数記録されている場合、予め設定された優先順位により前記認証方法に用いる認証用データを選択することを特徴とする請求項１から請求項３のいずれかに記載のＩＣカード。
【請求項５】　前記本人認証手段は、
認証の失敗により、前記認証データが使用停止となっても、他の認証データを用いた本人認証により本人を確認できる場合、使用停止となった該認証データを復元する手段を更に含むことを特徴とする請求項１から請求項４のいずれかに記載のＩＣカード。
【請求項６】　請求項１から請求項５のいずれかに記載のＩＣカードに、認証データを含む認証情報を登録する認証情報登録装置であって、
ＩＣカードが認証情報登録装置を正当な接続先であると確認するための登録認証を実行する登録認証手段と、
前記登録認証が正常な場合、登録可能な認証方法を表示し、利用者に希望する前記認証方法を選択させる選択手段と、
選択された前記認証方法と前記認証情報を前記ＩＣカードへ登録する登録手段と、
を設けたことを特徴とする認証情報登録装置。
【請求項７】　請求項１から請求項５のいずれかに記載のＩＣカードに、ＩＣカードで実行するアプリケーションプログラムを登録するアプリケーションプログラム登録装置であって、
アプリケーション用鍵によりアプリケーションプログラムの認証を実行する認証手段と、
前記アプリケーション鍵による認証が正常な場合、ＩＣカードに登録された認証方法により本人認証を行わせる確認手段と、
ＩＣカードが実行した本人認証が正常な場合、追加可能なアプリケーションプログラムを表示して、利用者に希望するするアプリケーションプログラムを選択させる選択手段と、
選択されたアプリケーションプログラムを登録・削除する登録・削除手段と、
を設けたことを特徴とするアプリケーションプログラム登録装置。
【請求項８】　請求項１から請求項５のいずれかに記載のＩＣカードを用いたサービス提供システムであって、
ＩＣカードの発行と利用者の管理を行う顧客管理サーバと、
利用者がＩＣカードを利用するための、自宅、あるいは店舗に用意されたクライアント端末と、
を設けたことを特徴とするサービス提供システム。
【請求項９】　利用者が街頭でＩＣカードを入手するためのＩＣカード自動販売機と、
ＩＣカード自動販売機の販売履歴と利用者を管理するＩＣカード販売管理サーバと、
を更に設けたことを特徴とする請求項８に記載のサービス提供システム。

【請求項１０】　ＩＣカード上に記録されたアプリケーションプログラムによりサービスを提供するＩＣカードにおけるＩＣカード使用者の認証方法であって、
前記ＩＣカードで実行される複数の前記アプリケーションプログラム、及び前記アプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録するＩＣカード上の記録手段に記録された認証方法を用いて、前記記録手段に記録された本人を特定する認証用データと、前記記録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりＩＣカード使用者の認証を行う本人認証処理と、
前記本人認証処理において認証が行われることにより前記記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行処理と、
を含むことを特徴とするＩＣカード使用者の認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、人間の生体情報による認証を含む、複数の認証方法を利用するＩＣカード、登録装置、及びサービス提供システムに関する。
【０００２】
【従来の技術】従来、本人の生体的特徴を利用して、本人を電子的に認証する技術の一つにバイオメトリクス技術がある。認証方法は、主に以下のように行う。
（１）あらかじめ本人の生体的特徴（経年変化が少なく、個人毎に特有の特徴があるもの）をディジタル化し登録する。
（２）照合時に認証する人の生体的特徴をスキャナなどで取り込みディジタル化し、あらかじめ登録したデータとの類似度を計算し、類似度が一定以上の場合、本人とする。
このようなバイオメトリクス技術をシステムに導入する際には、個人の生体情報を安全に管理する仕組みが必要である。なぜなら個人の生体情報は、プライバシー性の高い情報であり、変更ができないという特性を持っているからである。この問題を補完する一つの方法にＩＣカードなどの個人の携帯型機器と組み合わせる方法がある。すなわち、個人毎のＩＣカードに生体情報を格納し、管理させることで、プライバシーを守ることを可能とする。またＩＣカードに生体情報を格納し、小型の照合装置を組み合わせて使用することにより、認証サーバを利用せずにローカルで比較的安全な認証を可能とする技術も提案されている。これらの技術は、比較的少人数の場合であれば、小型の照合装置に複数人の生体情報を管理させる方法でシステム構築可能である。しかし、多人数で複数の照合装置を利用する場合、生体情報を一括管理することは難しい。そのため、個人毎のＩＣカードに生体情報を格納し、管理させる方法が提案されている。
【０００３】
【発明が解決しようとする課題】このような個人が所有する携帯機器の利用や、機器を用いて行う認証行為に対して、本人であるかを認証する方法には、パスワードを生体情報と組み合わせて利用するものがある。しかし、パスワードは、忘失による問題や盗難によるなりすましの危険性があるという問題があった。また、生体情報を利用する場合、怪我等の使用する部位の状態、体調、更には指紋認証を例に取ると、生まれつき指紋が薄くて認証には適さない等、生まれながらの特性により完全な本人認証ができない場合があるという問題があった。更に、これらの欠点を補完するためには複数の認証方法を組み合わせる必要がある。しかし、一般的に本人認証方法は、サービス提供者毎に固定的に決められている。そのため、本人認証をサービス毎に繰り返す必要があり、無駄が多いという問題があった。
【０００４】本発明は、上記問題点に鑑みてなされたもので、サービス提供者毎に別々の本人認証方法を用いるのではなく、複数のサービスから、ＩＣカード内の本人認証機能を共有することで、本人認証機能の無駄を省くことを可能とし、かつ、サービス利用者自身が複数の本人認証方法を、安全性を損なわない範囲で選択できる仕組みにより、本人認証に必要な情報の登録及び変更を容易に実現することを可能とするＩＣカード、登録装置、及びサービス提供システムを提供することを目的とする。
【０００５】
【課題を解決するための手段】上記問題点を解決するために、本発明は、ＩＣカード上に記録されたアプリケーションプログラムによりサービスを提供するＩＣカードであって、ＩＣカードで実行される複数のアプリケーションプログラム、及びアプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録する記録手段と、記録手段に記録された認証方法を用いて、記録手段に記録された本人を特定する認証用データと、記録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりＩＣカード使用者の認証を行う本人認証手段と、本人認証手段において認証が行われることにより記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行手段とを設けたことを特徴とする。以上の構成により、ＩＣカードで実行するアプリケーションプログラム、及びアプリケーションプログラムが要求する本人認証に必要な情報の登録及び変更を容易に実現することを可能とする。
【０００６】本発明は、上記ＩＣカードにおいて、本人認証手段は、認証方法の実行結果を予め設定された点数により取得する手段（例えば実施の形態のステップＳ１０２）と、予め設定された優先順位に従い実行される複

数の認証方法の実行結果として出力された点数を加算する手段（例えば実施の形態のステップＳ１０６）と、加算された点数とアプリケーションプログラムの指定する所定の点数とを比較する手段（例えば実施の形態のステップＳ１０３またはステップＳ１０７）とを更に含み、アプリケーションプログラムの指定する所定の点数を満たした時点で、アプリケーションに認証の正常終了を通知することを特徴とする。以上の構成により、ＩＣカードで実行されるアプリケーションプログラムの内容に関わらず、複数の認証方法を利用者が指定する優先順位により選択して実行することを可能とする。

【０００７】本発明は、上記ＩＣカードにおいて、本人認証手段は、認証方法の実行結果を予め設定された点数により取得する手段（例えば実施の形態のステップＳ１２３）と、認証方法の実行結果として出力された現在の点数と次に実行するアプリケーションプログラムの指定する所定の点数とを比較する手段（例えば実施の形態のステップＳ１２８からステップＳ１３０）と、比較の結果、アプリケーションプログラムの指定する所定の点数が現在の点数より大きい場合、アプリケーションプログラムに指定された認証方法を実行し、該認証方法による点数を新しい現在の点数として記録・更新する手段（例えば実施の形態のステップＳ１３１）とを更に含み、認証結果による現在の点数が、アプリケーションプログラムの指定する所定の点数を満たしていた場合、該アプリケーションプログラムの指定する認証方法の実行を省略することを特徴とする。以上の構成により、ＩＣカードで実行される複数のアプリケーションプログラムが認証方法の結果を共有することを可能とする。

【０００８】本発明は、上記ＩＣカードにおいて、本人認証手段は、認証に使用する認証用データが複数記録されている場合、予め設定された優先順位により認証方法に用いる認証用データを選択することを特徴とする。以上の構成により、怪我をして指紋認証ができない場合等に、認証方法の実行順序を変更することを可能とする。

【０００９】本発明は、上記ＩＣカードにおいて、本人認証手段は、認証の失敗により、認証データが使用停止となっても、他の認証データを用いた本人認証により本人を確認できる場合、使用停止となった該認証データを復元する手段（例えば実施の形態のステップＳ１４１からステップＳ１５３）を更に含むことを特徴とする。以上の構成により、利用者や管理者が安全かつ容易にＩＣカードの管理を行い、ＩＣカードを継続利用することを可能とする。

【００１０】本発明は、上記ＩＣカードに、認証データを含む認証情報を登録する認証情報登録装置であって、ＩＣカードが認証情報登録装置を正当な接続先であると確認するための登録認証を実行する登録認証手段（例えば実施の形態のステップＳ２）と、登録認証が正常な場合、登録可能な認証方法を表示し、利用者に希望する認証方法を選択させる選択手段（例えば実施の形態のステップＳ５からステップＳ６）と、選択された認証方法と認証情報をＩＣカードへ登録する登録手段（例えば実施の形態のステップＳ７）とを設けたことを特徴とする。以上の構成により、利用者がＩＣカードに希望する認証方法を安全かつ容易に登録することを可能とする。

【００１１】本発明は、上記ＩＣカードに、ＩＣカードで実行するアプリケーションプログラムを登録するアプリケーションプログラム登録装置であって、アプリケーション用鍵によりアプリケーションプログラムの認証を実行する認証手段（例えば実施の形態のステップＳ４３）と、アプリケーション鍵による認証が正常な場合、ＩＣカードに登録された認証方法により本人認証を行わせる確認手段（例えば実施の形態のステップＳ４５）と、ＩＣカードが実行した本人認証が正常な場合、追加可能なアプリケーションプログラムを表示して、利用者に希望するするアプリケーションプログラムを選択させる選択手段（例えば実施の形態のステップＳ４８からステップＳ４９）と、選択されたアプリケーションプログラムを登録・削除する登録・削除手段（例えば実施の形態のステップＳ５０）とを設けたことを特徴とする。以上の構成により、利用者がＩＣカードに希望するアプリケーションプログラムを安全かつ容易に登録することを可能とする。

【００１２】本発明は、上記ＩＣカードを用いたサービス提供システムであって、ＩＣカードの発行と利用者の管理を行う顧客管理サーバ（例えば実施の形態の顧客管理サーバ１０１）と、利用者がＩＣカードを利用するための、自宅、あるいは店舗に用意されたクライアント端末（例えば実施の形態のクライアント端末１０３）とを設けたことを特徴とする。以上の構成により、利用者がクライアント端末からの操作でＩＣカードの発行やＩＣカードの利用を行うことを可能とする。

【００１３】本発明は、上記サービス提供システムにおいて、利用者が街頭でＩＣカードを入手するためのＩＣカード自動販売機（例えば実施の形態のＩＣカード自動販売機１０５）と、ＩＣカード自動販売機の販売履歴と利用者を管理するＩＣカード販売管理サーバ（例えば実施の形態のＩＣカード販売管理サーバ１０６）とを更に設けたことを特徴とする。以上の構成により、利用者が街頭の端末からＩＣカードを入手することを可能とする。

【００１４】本発明は、ＩＣカード上に記録されたアプリケーションプログラムによりサービスを提供するＩＣカードにおけるＩＣカード使用者の認証方法であって、ＩＣカードで実行される複数のアプリケーションプログラム、及びアプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録するＩＣカード上の記録手段に記録された認証方法を用いて、記録手段に記録された本人を特定する認証用データと、記

録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりＩＣカード使用者の認証を行う本人認証処理と、本人認証処理において認証が行われることにより記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行処理とを含むことを特徴とする。

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について説明する。図１は、本実施の形態のＩＣカード上に構成される機能ブロックを説明するブロック図である。図１において、符号１は、本実施の形態のＩＣカードの動作を制御する制御処理部を示す。符号２は、制御処理部１とＩＣカードの情報を読み書きするＩＣカードのＲ／Ｗ（Read/Write）装置を接続する入出力制御部を示す。符号３は、ＩＣカード上で実行するアプリケーションプログラムや認証方法、及び認証用テンプレート（パスワードや認証用生体データ等のデータ）等を含む認証情報を記録するためのＥＥＰＲＯＭ（Electricaly Erasable and Programmable ROM ：電気的書き換え可能な不揮発性メモリ）を示す。符号４は、制御処理部１で実行される本実施の形態のＩＣカードの制御プログラムを予め記録してあるＲＯＭ（Read Only Memory）を示す。符号５は、制御処理部１で扱われる一時的なデータを記録するためのＲＡＭ（Random Access Memory）を示す。なお、本実施の形態のＩＣカードとＩＣカードのＲ／Ｗ装置とのインターフェースは接触型のみでなく、無線等を用いた非接触型により実現することも可能であり、この場合、入出力制御部２は無線系の回路を含むものとする。また、ＥＥＰＲＯＭ３は、フラッシュメモリ（Flash Memory：電気的書き換え可能な半導体不揮発性メモリ）を用いても良い。

【００１６】また、制御処理部１は、アプリケーション追加・削除機能部１１と、データ読み・書き処理部１２と、コマンド実行管理部１３と、本人認証機能部１４とから構成されている。アプリケーション追加・削除機能部１１は、ＥＥＰＲＯＭ３に記録されるアプリケーションプログラムの追加、及び削除を管理する。データ読み・書き処理部１２は、ＥＥＰＲＯＭ３に記録される認証方法や認証用テンプレート（パスワードや認証用生体データ等のデータ）等を含む認証情報の登録、及びメンテナンスを行う。コマンド実行管理部１３は、アプリケーション追加・削除機能部１１によりＩＣカード上に記録されたアプリケーションプログラムの処理を実行する。本人認証機能部１４は、ＥＥＰＲＯＭ３に記録された認証方法を用いて、ＥＥＰＲＯＭ３に記録された本人を特定する認証用テンプレート（パスワードや認証用生体データ等のデータ）と、コマンド実行管理部１３がアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりＩＣカード使用者の認証を行う。

【００１７】次に、図２、及び図３を用いてＥＥＰＲＯＭ３に記録される情報の構成を説明する。図２、及び図３は、本発明の実施の形態のＩＣカード上のＥＥＰＲＯＭ３に記録される情報の構成を説明する模式図である。図２、及び図３において、ＥＥＰＲＯＭ３に記録される情報の種類は大別すると次のように分類される。

（１）アプリケーションプログラム

（２）認証方法に関する情報

（３）鍵データ

（４）その他情報

それぞれについて更に詳細に説明すると、（１）アプリケーションプログラムとしては、”アプリケーションプログラム１～N”と、アプリケーションプログラムそれぞれについて、アプリケーションプログラムが本人認証機能部１４による認証機能を使用するか否かを示した”ａ．本人認証機能使用フラグ”と、アプリケーションプログラムが必要な本人認証のレベルを意味する”ｂ．本人確認レベル”が記録可能である。なお、”本人確認レベル”についての詳細は後述する。また、（２）認証方法に関する情報としては、認証方法１～Nのそれぞれについて、Ｍ個の”本人認証用テンプレート（パスワードや認証用生体データ等のデータ）”と、認証方法のパラメータとして、”しきい値、テンプレート優先順位、各テンプレートのロック・アンロック再試行回数、アンロック回数上限値、ロック回数上限値、組み合わせパラメータ”等が記録可能である。ここで、”しきい値”は、本人認証の際に入力されたテンプレートと、あらかじめカード内に設定したテンプレートとの類似度を算出し、その値がある値以上か否かにより、本人か否かを判断する時に利用する基準値である。”テンプレート優先順位”は、各々の本人認証方法で利用するテンプレートを、複数ＩＣカード内に格納する場合に、どのテンプレートを優先的に使用するかというパラメータである。なお、当該テンプレートは、１人のものを複数入れるだけでなく、複数人のテンプレートを入れてもよい。”組み合わせパラメータ”は、一度に複数のテンプレートを本人認証の際に使用する場合、その組み合わせ方法を示すパラメータである。

【００１８】更に、入力されたテンプレートと登録されているテンプレートを比較し、認証が失敗した回数をカード内に記録する。”ロック回数上限値”を越えて認証が失敗すると、当該テンプレートをロックし、当該テンプレートを使用できない状態にする。また”ロック再試行回数”は、”ロック回数上限値”から認証が失敗した数を引いた残り回数を示し、ロックまでの再試行可能回数を表す。なお、ロックをしない設定にするには、「ロック回数上限値」をゼロにすることにより可能とする。また、生体状態の変化により、仮に一つのテンプレートが「ロック回数上限値」を超えて、ロックした場合で

も、他のテンプレートで本人認証がＯＫになった場合、当該テンプレートをアンロックし、再度使用可能にすることができることとする。”アンロック回数上限値”は、アンロックが可能な上限回数を示し、一度アンロックをすると、”アンロック再試行回数”を１ずつ減少し、０になった段階でアンロックを実行不可能とする。また（３）鍵データとしては、アプリケーションプログラムを追加する際に使用する”アプリケーション追加用鍵データ”と、アプリケーションプログラムを削除する際に使用する”アプリケーション削除用鍵データ”と、ＩＣカード発行者がＩＣカード内のメンテナンスを行う際に使用する”発行者用鍵データ”と、ＩＣカード管理者がＩＣカード内のメンテナンスを行う際に使用する”メンテナンス用鍵データ”等が記録可能である。また、（４）その他情報としては、アプリケーションプログラムが実行した本人認証の結果である”カード側本人確認レベル”と、ＩＣカード内に設定している複数の認証方法の一覧を示す”カード側認証方法リスト”と、複数の認証方法が設定されている場合に、複数の認証方法を行う順番を示した”認証方法優先順位”とＩＣカードの有効期限を示す”カード有効期限”等が記録可能である。なお、カード側本人確認レベル”は本人認証が成功した段階でセットされ、ＩＣカードをリセットした段階でクリアされる。

【００１９】次に、図面を用いて、本実施の形態の動作を説明する。まず、図４のフローチャートを用いて、専用の登録端末によるＩＣカードへの本人認証機能の登録動作を説明する。図４において、まずユーザのＩＣカード入手意志を確認する（ステップＳ１）。ステップＳ１において、ユーザにＩＣカード入手の意志がある場合（ステップＳ１のＹＥＳ）、ＩＣカードに個人の認証データ（パスワードや生体情報など）を登録するためのＩＣカードの登録認証を実行する（ステップＳ２）。登録認証は、ＩＣカードが登録端末を正当な接続先であると確認するために行い、カードへの書き込みは、認証が成功した段階で可能となる。なお、認証動作の詳細は後述する。次に、ＩＣカードの登録認証が正常に終了したか否かを判定する（ステップＳ３）。ステップＳ３において、ＩＣカードの登録認証が正常に終了していた場合（ステップＳ３のＹＥＳ）、認証方法の登録を開始する（ステップＳ４）。そして、ユーザ自身が複数の認証方法の中から、適当な認証方法を選択できるように、登録可能な認証方法を表示する（ステップＳ５）。例えば、複数のスキャナやカメラなどがついている登録端末の場合、複数の認証方法をユーザ自身が選択することができる。次に、ユーザに希望の認証方法があるか否かを判断させる（ステップＳ６）。ステップＳ６において、ユーザが希望の認証方法があると判断した場合（ステップＳ６のＹＥＳ）、認証情報を登録する（ステップＳ７）。認証情報は、スキャナやカメラなどを用いて得た情報から特徴情報を抽出し、特徴情報の品質が良いと判断した段階で成功とし、当該データをＩＣカードへ書き込む。そして、認証情報の登録が成功したか否かを判定し（ステップＳ８）、登録が成功していたた場合（ステップＳ８のＹＥＳ）、カード内の認証方法リストを書き換え、ＩＣカードを排出して（ステップＳ９）、ＩＣカードへの本人認証機能の登録動作を終了する。

【００２０】一方、ステップＳ３において、ＩＣカードの登録認証が正常に終了していなかった場合（ステップＳ３のＮＯ）、ＩＣカードは偽造されていると判断し、システムを停止してカード発行動作を停止する（ステップＳ１０）。また、ステップＳ７において、認証情報の登録が成功していなかった場合（ステップＳ８のＮＯ）、再度登録するか否かをユーザに入力させる（ステップＳ１１）。ステップＳ１１において、再度登録するとユーザが入力した場合（ステップＳ１１のＹＥＳ）、ステップＳ５へ戻り、上述の動作を繰り返す。ステップＳ１１において、再度登録しないとユーザが入力した場合（ステップＳ１１のＮＯ）、ＩＣカードへの本人認証機能の登録動作を終了する。上述のように、登録の際には複数回の中から良い状態のものを選択して登録する。登録が失敗する場合は、ステップＳ５へ戻り、登録可能な認証方法を選択する。ここでは、認証方法の詳細を設定することも可能である。たとえば複数の認証方法を使う場合の順番や方法の組み合わせ方、テンプレートの順番や組み合わせ方である。また、使用したい認証方法の優先順位も設定できる。更に、上述の方法では、カード入手時に認証方法が設定されていないが、入手時点であらかじめ既に認証方法が設定されていても良い。その場合ＩＣカードへの登録認証の前に、設定された認証方法による照合を行い、認証が成功した段階で認証方法の追加・削除・優先順位の変更を可能とする。認証が失敗した場合はカードを排出する。

【００２１】次に、図５のシーケンス図を用いて、本人認証機能の登録時のＩＣカードへの登録認証動作の一例を説明する。登録認証動作は、まず登録端末からＩＣカードへ乱数生成要求を送信する（ステップＳ２１）。乱数生成要求を受信したＩＣカードは乱数を生成し（ステップＳ２２）、生成した乱数Ａを登録端末へ送信する（ステップＳ２３）。登録端末では乱数Ａを秘密鍵で暗号化し（ステップＳ２４）、ＩＣカードへ送信する（ステップＳ２５）。ＩＣカードでは、受信した暗号文を復号化し（ステップＳ２６）、復号化した乱数を生成した乱数Ａと比較する（ステップＳ２７）。比較の結果、乱数が一致した場合、登録フラグを立てて（ステップＳ２８）、登録端末へ正常終了を返信する（ステップＳ２９）。また、比較の結果、乱数が一致しない場合、登録端末へエラーを返信する（ステップＳ３０）。

【００２２】次に、図６のフローチャートを用いて、専用のアプリケーション登録・削除端末によるＩＣカード

へのアプリケーションプログラムの登録・削除動作を説明する。図６において、まずアプリケーション登録・削除端末にＩＣカードを挿入させる（ステップＳ４１）。次に、挿入されたＩＣカードの有効期限が期限内か否かを判定する（ステップＳ４２）。ステップＳ４２において、ＩＣカードが有効期限内であった場合（ステップＳ４２のＹＥＳ）、アプリケーション鍵による認証を行う（ステップＳ４３）。なお、アプリケーション鍵による認証の詳細は後述する。そして、認証が成功したか否かを判定し（ステップＳ４４）、認証が成功していれば（ステップＳ４４のＹＥＳ）、ＩＣカードに、図４に示した本人認証機能の登録により登録した本人認証を実行させる（ステップＳ４５）。次に、本人認証が成功したか否かを判定し（ステップＳ４６）、認証が成功していれば（ステップＳ４６のＹＥＳ）、ＩＣカード内に登録されている現在のアプリケーションプログラムの登録状況を表示する（ステップＳ４７）。また、追加可能なアプリケーションプログラムの一覧を表示する（ステップＳ４８）。次に、ユーザにアプリケーションプログラムの登録・削除を行うか否かを入力させ（ステップＳ４９）、ユーザがアプリケーションプログラムの登録・削除を行うと入力した場合（ステップＳ４９のＹＥＳ）、アプリケーションプログラムの登録・削除を行う（ステップＳ５０）。そして、アプリケーションプログラムの登録・削除が成功したか否かを判定し（ステップＳ５１）、成功していれば（ステップＳ５１のＹＥＳ）、ステップＳ４９へ戻り、更に、ユーザにアプリケーションプログラムの登録・削除を行うか否かを入力させる。

【００２３】一方、ステップＳ４２において、ＩＣカードが有効期限内でなかった場合（ステップＳ４２のＮＯ）、ＩＣカード内に登録してあるアプリケーション情報をセンタに送信し（ステップＳ５２）、再度ＩＣカードを入手する際に使用する。また、期限切れのＩＣカードは、カード内の本人確認用データを削除し、ソフトウェア的または、ハードウェア的にカードを再度使用できない状態にして廃棄する（ステップＳ５３）。

【００２４】また、ステップＳ４４においてアプリケーション鍵による認証が失敗であると判定した場合（ステップＳ４４のＮＯ）、ＩＣカード側またはシステム側の問題であるため、カード内のアプリケーション情報を読み出し、不正カード情報をセンタへ送信する（ステップＳ５４）。そして、カード内の登録や削除の鍵をロックさせ（ステップＳ５５）、ＩＣカードの排出を行う（ステップＳ５６）。更に、ステップＳ４９において、ユーザがアプリケーションプログラムの登録・削除を行わないと入力した場合（ステップＳ４９のＮＯ）、あるいは、ステップＳ５１において、アプリケーションプログラムの登録・削除が失敗したと判定した場合（ステップＳ５１のＮＯ）、ＩＣカードの排出を行う（ステップＳ５６）。なお、アプリケーションプログラムを追加する時点で、当該アプリケーションプログラム内にセットされている本人確認レベルが、カード側認証方法リストにない場合は、アプリケーションプログラムをダウンロードした直後にＩＣカードより、「ない」という意味のレスポンスをアプリケーション登録・削除端末に出しても良い。

【００２５】次に、図７と図８のシーケンス図を用いて、アプリケーションの登録・削除時のアプリケーション鍵による認証動作の一例を説明する。図７において、まず、アプリケーション登録・削除端末からＩＣカードへアプリケーションＩＤを送信する（ステップＳ６１）。次に、アプリケーションＩＤのチェックコードにより、ＩＣカード内に記録されているアプリケーションＩＤとの重複をチェックする（ステップＳ６２）。もし、チェックがＯＫの場合、ＩＣカード内にフラグを立てて（ステップＳ６３）、アプリケーション登録・削除端末へ正常終了を返信する（ステップＳ６４）。もし、チェックがＮＧの場合、アプリケーション登録・削除端末へエラーを返信する（ステップＳ６５）。次に、アプリケーション登録・削除端末からＩＣカードへ乱数生成要求を送信する（ステップＳ６６）。乱数生成要求を受信したＩＣカードは、乱数を生成し（ステップＳ６７）、生成した乱数Ｂをアプリケーション登録・削除端末へ送信する（ステップＳ６８）。

【００２６】乱数Ｂを受信したアプリケーション登録・削除端末は、乱数Ｂとアプリケーションプログラムのハッシュ値を秘密鍵で暗号化する（ステップＳ６９）。次に、暗号文とアプリケーションプログラム自身（アプリケーションプログラムの登録時のみ、削除時は暗号文のみ）をＩＣカードへ送信する（ステップＳ７０）。暗号文を受信したＩＣカードは、受信した暗号文を復号化し（ステップＳ７１）、復号化した乱数を生成した乱数Ｂと比較する（ステップＳ７２）。次に、図８において、アプリケーションプログラム登録時は、復号化したハッシュ値と送信されたアプリケーションプログラムのハッシュ値とを比較する（ステップＳ７３）。アプリケーションプログラム削除時は、復号化したハッシュ値とＩＣカード内に記録されたアプリケーションプログラムのハッシュ値とを比較する（ステップＳ７４）。そして、比較の結果、乱数Ｂ及びハッシュ値が一致する場合、アプリケーションプログラムの登録、または削除を実行する（ステップＳ７５）。比較の結果、乱数Ｂ及びハッシュ値が一致しない場合、アプリケーション登録・削除端末へエラーを返信する（ステップＳ７６）。

【００２７】次に、表１を用いて、本実施の形態のＩＣカード上で実行される認証方法毎の本人確認レベルの一例を説明する。”本人確認レベル”は、アプリケーションプログラムが必要とする本人認証のセキュリティレベルを意味する。

【表１】

認証方法	本人確認レベル
指紋照合 スコア６０％以上	１３
指紋照合 スコア４０％以上	８
指紋照合 スコア３０％以上	６
ＰＩＮ照会 完全一致	１０
ＰＩＮ照会 １桁間違い	１
ＰＩＮ照会 全桁間違い	－５
生年月日の入力	１
音声認証 スコア３０％以上	８
音声認証 スコア２０％以上	６
正当なカードかどうか チェックする	３

表１には、認証方法の種類と、それぞれについての本人確認レベルが１対１で記録されている。例を挙げて説明すると、指紋照合による認証方法において、スコアが６０％以上で指紋が一致するのは非常に厳しい条件となるので、その本人確認レベルは１３ポイントとして高く設定されている。また、生年月日のような情報は簡単に他人に知られてしまうので、生年月日の入力は本人確認レベルが１ポイントとして低く設定されている。このように本人確認レベルは、難易度で分類された認証方法毎にアプリケーションプログラムが必要とする本人認証のセキュリティレベルをポイントで表し、難易度が高い程、そのポイントも高く設定されている。

【００２８】以上を踏まえて、次に、図９のフローチャートを用いて、本実施の形態のＩＣカードで実行されるアプリケーションが１つの認証方法を実行する場合の動作を説明する。図９において、まず、アプリケーションが本人認証を要求する（ステップＳ８１）。次に、アプリケーションが要求する本人確認レベルをカード側本人確認機能へ送信し（ステップＳ８２）、カード内の認証方法が要求された本人確認レベルを満足するか否かを判定する（ステップＳ８３）。ステップＳ８３において、カード内の認証方法が要求された本人確認レベルを満足する場合（ステップＳ８３のＹＥＳ）、優先順位の高い認証方法を選択し（ステップＳ８４）、選択された認証方法が実行可能であるか否かを判定する（ステップＳ８５）。ステップＳ８５において、選択された認証方法が実行可能である場合（ステップＳ８５のＹＥＳ）、指定された認証方法を実行する（ステップＳ８６）。そして、認証が成功したか否かを判定する（ステップＳ８７）。ステップＳ８７において、指定された認証が成功していた場合（ステップＳ８７のＹＥＳ）、アプリケーションに結果を返信する（ステップＳ８８）。一方、ステップＳ８３において、カード内の認証方法が要求された本人確認レベルを満足しない場合（ステップＳ８３のＮＯ）、あるいは、ステップＳ８５において、選択された認証方法が実行不可能である場合（ステップＳ８５のＮＯ）、アプリケーションにエラーを返信し（ステップＳ８９）、アプリケーション利用サービスを終了する。また、ステップＳ８７において、指定された認証が成功していなかった場合（ステップＳ８７のＮＯ）、失敗を記録して（ステップＳ９０）、アプリケーションに結果を返信する（ステップＳ８８）。

【００２９】次に、図１０のフローチャートを用いて、本実施の形態のＩＣカードで実行されるアプリケーションが複数の認証方法を優先順位により選択して実行する場合の動作を説明する。図１０において、アプリケーションが本人認証を要求すると、優先順位１の認証方法を実行する（ステップＳ１０１）。次に、実行した認証方法の認証結果の本人確認レベルを求め、カード側本人確認レベルへ記録する（ステップＳ１０２）。次に、カード側本人確認レベルが、アプリケーションで要求された本人確認レベルを満たすか否かを判定する（ステップＳ１０３）。ステップＳ１０３において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たさないと判定した場合（ステップＳ１０３のＮＯ）、優先順位に従い、本人確認レベルを満たす最適な認証方法を探索する（ステップＳ１０４）。次に、探索回数が予め設定された上限値を超えたか否か判定し

（ステップＳ１０５）、探索回数が上限値を超えていない場合（ステップＳ１０５のＮＯ）、探索した認証方法を実行して認証結果の本人確認レベルを算出し、カード側本人確認レベルへ加算する（ステップＳ１０６）。そして、加算されたカード側本人確認レベルが、アプリケーションで要求された本人確認レベルを満たすか否かを判定する（ステップＳ１０７）。

【００３０】ステップＳ１０７において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たさないと判定した場合（ステップＳ１０７のＮＯ）、ステップＳ１０４へ戻り、上述の動作を繰り返して本人確認レベルを加算して積み重ねる。一方、ステップＳ１０５において、探索回数が予め設定された上限値を超えていた場合（ステップＳ１０５のＹＥＳ）、アプリケーションに認証エラーを通知して（ステップＳ１０８）終了する。また、ステップＳ１０３において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たすと判定した場合（ステップＳ１０３のＹＥＳ）、あるいは、ステップＳ１０７において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たすと判定した場合（ステップＳ１０７のＹＥＳ）、ＩＣカード内に現在の本人確認レベルを設定して（ステップＳ１０９）アプリケーションの実行を行う。なお、上述の説明では、ステップＳ１０４において、優先順位に従って本人確認レベルを満たす最適な認証方法を探索する場合、探索回数を予め設定し、探索回数が設定された上限値を超えたか否かを、探索を続けるか否かの判定基準としたが、探索回数と同様に探索時間を設定し、探索時間が設定された上限時間を超えたか否かを、探索を続けるか否かの判定基準としても良い。

【００３１】次に、図１１のフローチャートを用いて、本実施の形態のＩＣカードで実行される複数のアプリケーションが認証結果を共有する場合の動作を説明する。ここでは、複数のアプリケーションプログラムの中でユーザが最初に実行させるアプリケーションプログラムを”アプリケーション１”として説明を行う。図１１において、まず、ユーザにアプリケーション１を選択させる（ステップＳ１２１）。次に、アプリケーション１が要求するカード側本人認証機能により本人認証を行い（ステップＳ１２２）、認証結果をカード側本人確認レベルへ記録する（ステップＳ１２３）。認証結果を記録したら、アプリケーション１を実行する（ステップＳ１２４）。　次に、ユーザに続けて他のアプリケーションを実行するか否かを入力させる（ステップＳ１２５）。ステップＳ１２５において、ユーザが続けて他のアプリケーションを実行するとした場合（ステップＳ１２５のＹＥＳ）、他のアプリケーションを選択させる（ステップＳ１２６）。他のアプリケーションが選択されたら、他のアプリケーションが要求する認証方法を確認する（ステップＳ１２７）。次に、現在のカード側本人確認レベルを取得する（ステップＳ１２８）。現在のカード側本人確認レベルを取得したら、カード側本人確認レベルと他のアプリケーションに要求された本人確認レベルを比較し（ステップＳ１２９）、要求された本人確認レベルの方が大きいか否かを判定する（ステップＳ１３０）。

【００３２】ステップＳ１３０において、要求された本人確認レベルの方が大きい場合（ステップＳ１３０のＹＥＳ）、要求された認証方法による本人認証を行い、カード側本人確認レベルを更新する（ステップＳ１３１）。ここで、カード側本人確認レベルの更新は、”本人確認レベル（更新後）＝本人確認レベル（更新前）＋他のアプリケーションの認証結果による本人確認レベル”とする。また、ここでは単純に加算をした例を示しているが、利用環境によって予め設定されている重み付け因子を掛け合わせた値を加算しても良い。本人確認レベルが更新されたら、他のアプリケーションを実行し（ステップＳ１３２）、ステップＳ１２５に戻って、ユーザに更なる他のアプリケーションを実行するか否かを入力させる。一方、ステップＳ１２５において、ユーザが続けて他のアプリケーションを実行しないとした場合（ステップＳ１２５のＮＯ）、カード側本人確認レベルをクリアし（ステップＳ１３３）、アプリケーション利用サービスを終了する（ステップＳ１３４）。また、ステップＳ１３０において、要求された本人確認レベルの方が小さい場合（ステップＳ１３０のＮＯ）、要求された認証方法による本人認証は行わず、他のアプリケーションを実行する（ステップＳ１３２）。

【００３３】また、カード内の本人認証機能を使う場合、認証の失敗によりテンプレートがロックする場合がある。そこで、テンプレートがロックした場合においても、ユーザがカードを継続して利用できるよう、図１２、及び図１３のフローチャートを用いて、専用のメンテナンス装置によるＩＣカードのカード所持者が行う本人認証機能のメンテナンス動作を説明する。図１２において、まず、メンテナンス装置へＩＣカードを挿入させる（ステップＳ１４１）。次に、ＩＣカードメンテナンス認証を行う（ステップＳ１４２）。メンテナンス認証の方法は、図５で説明した認証方法をメンテナンス鍵により行うことが違うのみであるので、ここでは説明を省略する。メンテナンス認証を行ったら、認証が成功したか否かを判定する（ステップＳ１４３）。ステップＳ１４３において、メンテナンス認証が成功していた場合（ステップＳ１４３のＹＥＳ）、ＩＣカードに、ロックしていないテンプレートで本人認証を行わせる（ステップＳ１４４）。次に、本人認証が成功したか否かを判定する（ステップＳ１４５）。ステップＳ１４５において、本人認証が成功していた場合（ステップＳ１４５のＹＥＳ）、現在ロックしているテンプレートの一覧を表

示する（ステップＳ１４６）。
【００３４】ロックしているテンプレートの一覧を取得したら、アンロック可能なテンプレートがあるか否かを判定する（ステップＳ１４７）。ステップＳ１４７において、アンロック可能なテンプレートがある場合（ステップＳ１４７のＹＥＳ）、図１３に示すようにロックを解除する（ステップＳ１４８）。次に、ロックの解除が成功したか否かを判定する（ステップＳ１４９）。ステップＳ１４９において、ロックの解除が成功していた場合（ステップＳ１４９のＹＥＳ）、テンプレートの再登録を実行する（ステップＳ１５０）。テンプレートの再登録を実行したら、テンプレートの再登録が成功したか否かを判定し（ステップＳ１５１）、成功していた場合（ステップＳ１５１のＹＥＳ）、現在の登録状況を表示する（ステップＳ１５２）。そして、ＩＣカードのテンプレートの登録状況を表示したら、ＩＣカードを排出する（ステップＳ１５３）。
【００３５】一方、ステップＳ１４３において、メンテナンス認証が成功していなかった場合（ステップＳ１４３のＮＯ）、ＩＣカードを取り込み、システムを停止して終了する（ステップＳ１５４）。また、ステップＳ１４５において、本人認証が成功していなかった場合（ステップＳ１４５のＮＯ）、再度確認するか否かを確かめ（ステップＳ１５５）、再度確認する場合（ステップＳ１５５のＹＥＳ）、ステップＳ１４４へ戻り、本人認証を再実行させる。ステップＳ１５５において、本人認証を再度確認しない場合（ステップＳ１５５のＮＯ）、あるいは、ステップＳ１４７において、アンロック可能なテンプレートがない場合（ステップＳ１４７のＮＯ）、ステップＳ１５３へ進み、ＩＣカードを排出する。また、ステップＳ１５１において、テンプレートの再登録が成功していなかった場合（ステップＳ１５１のＮＯ）、再度、再登録するか否かを確認する（ステップＳ１５６）。ステップＳ１５６において、再登録を行う場合（ステップＳ１５６のＹＥＳ）、ステップＳ１５０へ戻り、上述の動作を繰り返す。ステップＳ１５６において、再登録を行なわない場合（ステップＳ１５６のＮＯ）、現在の登録状況を表示し（ステップＳ１５２）、ＩＣカードを排出する（ステップＳ１５３）。
【００３６】次に、図１４のフローチャートを用いて、専用のメンテナンス装置によるＩＣカードのシステム管理者が行う本人認証機能のメンテナンス動作を説明する。図１４において、まず、メンテナンス装置へ管理者ＩＣカードを挿入させる（ステップＳ１６１）。次に、ＩＣカードに、ロックしていないテンプレートで本人認証を行わせ（ステップＳ１６２）、本人認証が成功したか否かを判定する（ステップＳ１６３）。ステップＳ１６３において、本人認証が成功していた場合（ステップＳ１６３のＹＥＳ）、メンテナンス用の鍵を読み出す（ステップＳ１６４）。メンテナンス用鍵を取得したら、管理者ＩＣカードを排出し（ステップＳ１６５）、ユーザ用のＩＣカードを挿入させる（ステップＳ１６６）。そして、図１２に示したステップＳ１４２に進み、ステップＳ１４２からステップＳ１５６までの上述の動作を行う。一方、ステップＳ１６３において、本人認証が成功していなかった場合（ステップＳ１６３のＮＯ）、再度確認するか否かを確かめ（ステップＳ１６７）、再度確認する場合（ステップＳ１６７のＹＥＳ）、ステップＳ１６２へ戻り、本人認証を再実行させる。ステップＳ１６７において、本人認証を再度確認しない場合（ステップＳ１６７のＮＯ）、ＩＣカードを排出する（ステップＳ１６８）。
【００３７】（実施例の説明）次に、本発明の実施例を図面を参照して説明する。図１５は、本発明の実施例のシステム構成を説明するブロック図である。本実施例は、ＩＣカードを郵送や街角の自動販売機から入手する例を示す。図１５において、符号１０１は、ＩＣカードの発行とＩＣカードのユーザ管理を行う顧客管理サーバを示す。符号１０２は、認証データを登録してＩＣカードを発行する顧客管理サーバ１０１に接続された認証データ登録ＩＣカード発行機を示す。符号１０３は、ＩＣカードのユーザが顧客管理サーバへアクセスするためのクライアント端末を示す。符号１０４は、指紋情報等の認証用の情報を取得するためにクライアント端末１０３に接続されたスキャナまたは照合装置を示す。符号１０５は、現金の支払い機能の他に、カメラや指紋照合装置、暗証番号入力用の操作部等を備えたＩＣカード自動販売機を示す。ＩＣカード自動販売機では、個人がカードを購入する時には、必ずなんらかの認証方法を選択しなければＩＣカードは購入できないものとする。符号１０６は、ＩＣカード自動販売機で販売されたＩＣカードの情報を管理するＩＣカード販売管理サーバを示す。符号１０７は、顧客管理サーバ１０１と、クライアント端末１０３と、ＩＣカード自動販売機１０５と、ＩＣカード販売管理サーバ１０６との間を接続するコンピュータネットワークを示す。なお、クライアント端末１０３は、スキャナ、または照合装置が接続できればＰＣ等の他、携帯端末でも良い。
【００３８】次に、図１６に示すシーケンス図を用いて、図１５に示すシステムにおける認証データ登録ＩＣカード発行機１０２によるＩＣカード発行動作を説明する。図１６において、まず、個人の自宅のパソコン（クライアント端末１０３）からダイアルアップでプロバイダなどに接続し、インターネット上の顧客管理サーバ１０１が立ち上げているホームページに接続する。そして、認証機能登録のセッションを要求する（ステップＳ１８１）。セッションを要求された顧客管理サーバ１０１は、認証情報の入力をクライアント端末１０３を操作するユーザへ求める（ステップＳ１８２）。認証情報の入力を要求されたユーザは、クライアント端末１０３か

らＩＤ番号やパスワード等を送信する（ステップＳ１８３）。顧客管理サーバ１０１では、送信された認証情報によりユーザの認証を行い（ステップＳ１８４）、結果をクライアント端末１０３へ通知する（ステップＳ１８５）。認証結果を受けて、ユーザは次にクライアント端末１０３から、自分の氏名、電話番号の他、メールアドレス、ＩＣカードの登録に必要な暗証番号などのパスワード等のＩＣカードへの記録情報、本人が確認できる画像データ（運転免許証や保険証のコピー）や電子証明書等を送信する（ステップＳ１８６）。このときに、登録するＩＣカードの種類や、価格、絵柄、メモリ容量を選択できるようにしても良い。また、ＩＣチップとカードが分離できる場合は、バラバラに購入し、使用時に組み合わせても良い。

【００３９】ＩＣカードへの記録情報を受信した顧客管理サーバ１０１は、発信者番号通知により取得した電話番号や氏名と、入力された電話番号や氏名が一致することを確認してユーザを確認する（ステップＳ１８７）。ユーザが確認できたら、顧客管理サーバ１０１は、認証データ登録ＩＣカード発行機１０２へ、顧客管理サーバ１０１で受信した本人が確認できる情報や画像、更にパスワード等のＩＣカードへの記録情報を送信する（ステップＳ１８８）。次に、クライアント端末へ認証情報の登録の確認として、登録応答を送信する（ステップＳ１８９）。一方、認証データ登録ＩＣカード発行機１０２は、顧客管理サーバ１０１から送信された認証情報等のデータを記録したＩＣカードを発行し、顧客管理サーバ１０１に履歴を登録する（ステップＳ１９０）。その後、発行されたＩＣカードは郵送等によりクライアント端末１０３を操作するユーザの元へ届けられ（ステップＳ１９１）、ユーザは必要に応じて本人認証データの再登録を行う（ステップＳ１９２）。送付されたＩＣカードは、指定した暗証番号や、画像データが登録されているので、それらを用いて本人認証した後に、個人が選択する認証方法で、再登録することができる。例えば、自宅のパソコンに接続した本人認証装置から取り込んだ指紋データをＩＣカードに再登録することで、指紋によるカード所持者確認も可能となる。なお、再登録の手続きは、個人が選択できる認証方法を一度しか変更できない設定にさせても良い。また、クライアントサーバ間でやり取りを行うデータは暗号化されていても良い。

【００４０】次に、図１７に示すシーケンス図を用いて、図１５に示すシステムにおけるＩＣカード自販機によるＩＣカード入手動作を説明する。図１７において、まず、ユーザが街角にあるＩＣカード自動販売機１０５に行き、ＩＣカードの購入を要求する（ステップＳ２０１）。ユーザにＩＣカードの購入を要求されたＩＣカード自動販売機１０５は、ＩＣカード販売管理サーバ１０６へカード登録のセッションを要求する（ステップＳ２０２）。カード登録のセッションを要求されたＩＣカード販売管理サーバ１０６は、ＩＣカード自動販売機１０５へセッションの要求応答を送信する（ステップＳ２０３）。ＩＣカード販売管理サーバ１０６のセッション要求応答を受信したＩＣカード自動販売機１０５は、ユーザへＩＣカード購入要求の応答を表示する（ステップＳ２０４）。次に、ユーザはＩＣカードに設定する認証方法を選択し（ステップＳ２０５）、必要な認証データ等のＩＣカードへの記録情報を入力する（ステップＳ２０６）。ＩＣカードへの記録情報を受信したＩＣカード自動販売機１０５は、ＩＣカードの発行・登録を行い（ステップＳ２０７）、発行したＩＣカード情報をＩＣカード販売管理サーバ１０６へ送信する（ステップＳ２０８）。ＩＣカードの発行・登録情報を受信したＩＣカード販売管理サーバ１０６は、ＩＣカード自動販売機１０５へカード登録のセッション終了を送信する（ステップＳ２０９）。そして、ＩＣカード自動販売機１０５は、作成されたＩＣカードを排出して（ステップＳ２１０）ＩＣカード販売の動作を終了する。

【００４１】次に、このようにして入手したＩＣカードの使用例を図面を用いて説明する。本使用例は、病気を患っているユーザが、遠い病院に薬をとりに行く手間は非常に大変であるので、病院が患者の住んでいる場所の近くのコンビニエンスストアに、当該患者の薬を運ぶサービスを行う例である。ＩＣカード内には、ＩＣカードにキャッシュカードアプリケーションが既に入っており、上記サービスを受けたい利用者は、病院等で病院のＩＤカードアプリケーションを入手し、近くのコンビニへ薬を取りにいく。まず、図１８から図２１にＩＣカード内のデータ構成の例を示す。図１８は、本発明の実施例のＩＣカード内アプリケーション構成例を説明する模式図である。図１８において、ＩＣカード内には、（１）アプリケーションプログラムとして、”キャッシュカードアプリケーション”と後からダウンロードされた”病院用ＩＤカードアプリケーション”が記録されている。それぞれのアプリケーションには、”ａ．本人認証機能使用フラグ”と、”ｂ．本人確認レベル”が設定されており、病院用ＩＤカードアプリケーションには、更に”ｃ．薬情報”が記録されている。

【００４２】また、（２）認証方法に関する情報として、認証方法１を順位１、認証方法３を順位２、認証方法２を順位３とする”認証方法優先順位”と、認証方法１をパスワード、認証方法２を指紋照合、認証方法３を音声照合とする”カード側認証方法リスト”と、認証方法１のテンプレート及びパラメータと、認証方法２のテンプレート及びパラメータと、認証方法３のテンプレート及びパラメータが記録されている。図１９は、図１８におけるＩＣカード内のパスワードによる認証方法リストの詳細を説明する模式図である。図２０は、図１８におけるＩＣカード内の指紋照合による認証方法リストの詳細を説明する模式図である。図２１は、図１８におけ

るＩＣカード内の音声照合による認証方法リストの詳細を説明する模式図である。各図において、それぞれの認証方法は、”ａ．認証方法用テンプレート”と、更に”ｂ．認証方法パラメータ”として、”しきい値”、”テンプレート優先順位”、”ロック再試行回数”、”アンロック再試行回数”、”アンロック回数上限値”、”ロック回数上限値”、”組み合わせパラメータ”の各パラメータが設定されている。上述の例では、ユーザが手を怪我しており指紋認証ができないの状況が生じたため、指紋認証の順位を一番後ろになるように設定されている。

【００４３】以上を前提に、本実施例の実施方法を示す。図２２、及び図２３は、ＩＣカードに記録された病院用ＩＤカードアプリケーションの動作を説明するシーケンス図である。図２２において、まず、ユーザは自宅に用意されたクライアント端末１０３により、病院のホームページへアクセスし、ＩＣカードを挿入して病院用アプリケーション（病院のホームページ）に薬購入のセッションを要求する（ステップＳ２２１）。病院用アプリケーションは、セッション要求に応答してＩＣカード（病院用ＩＤカードアプリケーション）に相互認証を要求する（ステップＳ２２２）。次に、ＩＣカードと病院用アプリケーションは相互認証を行う（ステップＳ２２３）。なお、相互認証の詳細は後述する。相互認証が終了したら、病院用ＩＤカードアプリケーションによる本人認証を行う（ステップＳ２２４）。ここでは、病院用ＩＤカードアプリケーションが要求する本人確認レベルが、指紋認証、または音声認証とパスワードの併用のどちらか一方が必要であるため、上述のようにＩＣカード内の優先順位の高い、パスワードと音声認証の併用を本人認証方法として選択する。当該認証方法にて本人確認を行い、認証が成功した段階で、病院内のホームページにログインができ、必要な薬の購入を病院のホームページから注文する（ステップＳ２２５）。

【００４４】次に、病院用アプリケーションは、薬の在庫チェックを行い（ステップＳ２２６）、在庫が確認できれば購入代金の支払いを要求する（ステップＳ２２７）。購入代金の支払いを要求されたユーザは、キャッシュカードアプリケーションによる支払処理を行う（ステップＳ２２８）。なお、キャッシュカードアプリケーションによる支払処理の詳細は後述する。キャッシュカードアプリケーションによる支払処理後、ユーザは支払要求に対する応答を行い（ステップＳ２２９）、病院用アプリケーションは、ＩＣカードに薬の予約情報を書き込む（ステップＳ２３０）。ＩＣカードから予約情報書き込みに対する応答が送信されると（ステップＳ２３１）、病院用ＩＤカードアプリケーションは、指定の店舗への薬の配送を行う（ステップＳ２３２）。

【００４５】後日、ユーザは指定の店舗へ行き、店舗に用意されたクライアント端末１０３に対して薬購入のセッションを要求する（ステップＳ２３３）。店舗端末（店舗用のアプリケーション）は、セッション要求に応答してＩＣカードに相互認証を要求する（ステップＳ２３４）。次にＩＣカードと店舗端末は相互認証を行う（ステップＳ２３５）。なお、相互認証の詳細は後述する。相互認証が終了したら、図２３に示すように、薬の受け取りに必要な本人認証を行う（ステップＳ２３６）。ここでは、薬の受け取りに必要な本人確認レベルは、低く設定されているため、カードを持っていることによって本人認証がなされる。次に、店舗端末は薬の予約情報をＩＣカードへ送信し（ステップＳ２３７）、ＩＣカードは、カード側に登録されている薬情報と、届けられている薬との整合性を確認する（ステップＳ２３８）。そして、確認結果を店舗端末へ通知する（ステップＳ２３９）と同時に、店舗はカード所有者に当該の薬を手渡す（ステップＳ２４０）。なお、カード側に登録されている薬情報と、届けられている薬との整合性を確認できたら、ＩＣカードは予約情報は削除する。

【００４６】次に、図２４、及び図２５のシーケンス図を用いて、ＩＣカードと病院または店舗用のアプリケーションとの相互認証動作の一例を説明する。図２４において、まず、病院または店舗用のアプリケーションが、アプリケーション鍵を発行者鍵により暗号化し（ステップＳ２４１）、ＩＣカードへ送信する（ステップＳ２４２）。ＩＣカードは受信した暗号文を復号化し、アプリケーション鍵をＩＣカードにセットする（ステップＳ２４３）。次に、病院または店舗用のアプリケーションは乱数Ｃを発生し（ステップＳ２４４）、ＩＣカードへ生成した乱数Ｃを送信する（ステップＳ２４５）。乱数Ｃを受信したＩＣカードは、アプリケーション鍵で乱数Ｃを暗号化し（ステップＳ２４６）、病院または店舗用のアプリケーションへ送信する（ステップＳ２４７）。病院または店舗用のアプリケーションは、受信した暗号文を復号化し（ステップＳ２４８）、復号化した乱数を生成した乱数Ｃと比較する（ステップＳ２４９）。ステップＳ２４９において、比較した乱数が一致した場合、病院または店舗用のアプリケーションは、アプリケーション鍵はＩＣカードにセットされたと判断する（ステップＳ２５０）。ステップＳ２４９において、比較した乱数が一致しない場合、病院または店舗用のアプリケーションは、アプリケーション鍵はＩＣカードにセットされないと判断する（ステップＳ２５１）。アプリケーション鍵がＩＣカードにセットされない場合、ＩＣカードは偽造である可能性がある。

【００４７】次に、図２５に示すように、ＩＣカードが、カード鍵を発行者鍵により暗号化し（ステップＳ２５２）、病院または店舗用のアプリケーションへ送信する（ステップＳ２５３）。病院または店舗用のアプリケーションは受信した暗号文を復号化し、カード鍵を病院または店舗用のアプリケーションにセットする（ステッ

プＳ２５４）。次に、ＩＣカードは乱数Ｄを発生し（ステップＳ２５５）、病院または店舗用のアプリケーションへ生成した乱数Ｄを送信する（ステップＳ２５６）。乱数Ｄを受信した病院または店舗用のアプリケーションは、カード鍵で乱数Ｄを暗号化し（ステップＳ２５７）、ＩＣカードへ送信する（ステップＳ２５８）。ＩＣカードは、受信した暗号文を復号化し（ステップＳ２５９）、復号化した乱数を生成した乱数Ｄと比較する（ステップＳ２６０）。ステップＳ２６０において、比較した乱数が一致した場合、ＩＣカードは、カード鍵は病院または店舗用のアプリケーションにセットされたと判断する（ステップＳ２６１）。ステップＳ２６０において、比較した乱数が一致しない場合、ＩＣカードは、カード鍵は病院または店舗用のアプリケーションにセットされないと判断する（ステップＳ２６２）。カード鍵が病院または店舗用のアプリケーションにセットされない場合、病院または店舗用のアプリケーションは盗聴や改竄がされている可能性がある。

【００４８】次に、図２６のシーケンス図を用いて、本実施例のＩＣカードのキャッシュカードアプリケーションの動作を説明する。図２６において、、まず、ユーザは自宅に用意されたクライアント端末１０３により、銀行用アプリケーションを起動し、ＩＣカードを挿入してキャッシュカードアプリケーションによる銀行決済のセッションを要求する（ステップＳ２８１）。銀行用アプリケーションは、セッション要求に応答してＩＣカードに本人認証を要求する（ステップＳ２８２）。ただし、ここでの本人確認は、既に病院用ＩＤカードアプリケーションでの本人確認結果がカード内に存在しているため、図１１のステップＳ１３０の手順に従えば、ここでの本人確認は省略が可能である。ＩＣカードは正常に認証されたら、銀行用アプリケーションにステータスを送信する（ステップＳ２８３）。次に、銀行用アプリケーションはＩＣカードの情報読み出しを行う（ステップＳ２８４）。ＩＣカードは情報の読み出しに応答して、ユーザの口座情報や信用情報を銀行端末へ送信する（ステップＳ２８５）。この時、送信する情報は暗号化しても良い。次に、銀行用アプリケーションは、銀行端末へ振込先情報を送信する（ステップＳ２８６）。ユーザの情報と振込先情報を受信した銀行端末は、口座振替処理を行い（ステップＳ２８７）、振替結果をＩＣカードへ通知する（ステップＳ２８８）。口座振替通知を受信したＩＣカードは、口座振替結果を記録し（ステップＳ２８９）、銀行用アプリケーションへステータスを送信して（ステップ２９０）、ＩＣカードのキャッシュカードアプリケーションを終了する。

【００４９】次に、図２７のフローチャートを用いて、本実施例のようにＩＣカード内に２つのテンプレートが存在する場合のテンプレート選択動作を説明する。図２７において、まず、第１テンプレートを用いて本人認証を行う（ステップＳ３０１）。次に、認証が成功したか否かを判定する（ステップＳ３０２）。ステップＳ３０２において、認証が成功していなかった場合（ステップＳ３０２のＮＯ）、第１のテンプレートによる認証回数を示すカウンタがＮ以上か否かを判定する（ステップＳ３０３）。ステップＳ３０３において、カウンタがＮ未満であった場合（ステップＳ３０３のＮＯ）、ステップＳ３０１へ戻り、上述の第１テンプレートによる本人認証を繰り返す。ステップＳ３０３において、カウンタがＮ以上であった場合（ステップＳ３０３のＹＥＳ）、次のテンプレートによる認証を行うか否かをユーザに入力させる（ステップＳ３０４）。ステップＳ３０４において、ユーザが次のテンプレートによる認証を行うとした場合（ステップＳ３０４のＹＥＳ）、第２テンプレートを用いて本人認証を行う（ステップＳ３０５）。次に、認証が成功したか否かを判定する（ステップＳ３０６）。ステップＳ３０６において、認証が成功していなかった場合（ステップＳ３０６のＮＯ）、第２のテンプレートによる認証回数を示すカウンタがＮ以上か否かを判定する（ステップＳ３０７）。ステップＳ３０７において、カウンタがＮ未満であった場合（ステップＳ３０７のＮＯ）、ステップＳ３０５へ戻り、上述の第２テンプレートによる本人認証を繰り返す。ステップＳ３０７において、カウンタがＮ以上であった場合（ステップＳ３０７のＹＥＳ）、本人認証の失敗を記録し（ステップＳ３０８）、アプリケーションに結果を返す（ステップＳ３０９）。一方、ステップＳ３０２において、認証が成功していた場合（ステップＳ３０２のＹＥＳ）、ステップＳ３０８へ進み、アプリケーションに結果を返す。また、ステップＳ３０６において、認証が成功していた場合も（ステップＳ３０６のＹＥＳ）、ステップＳ３０８へ進み、アプリケーションに結果を返す。

【００５０】

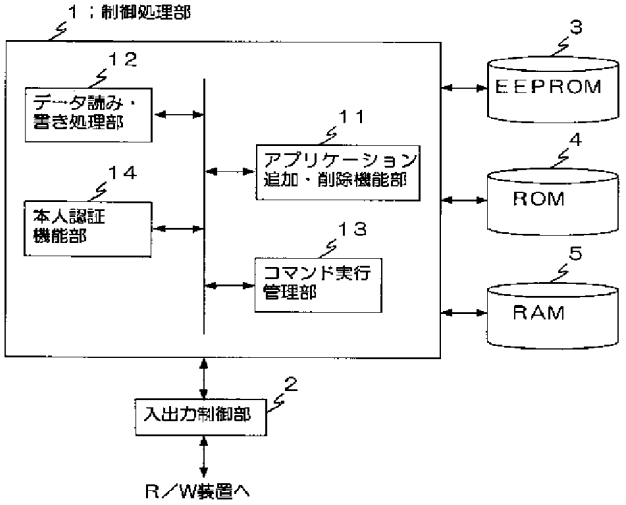
【発明の効果】以上の如く本発明によれば、サービス提供者毎に別々の本人認証方法を用いるのではなく、複数のサービスから、ＩＣカード内の本人認証機能を共有することで、本人認証機能の無駄を省くことが可能となり、かつ、サービス利用者自身が複数の本人認証方法を、安全性を損なわない範囲で選択できる仕組みにより、本人認証に必要な情報の登録及び変更を容易に実現することが可能となる。従って、認証に対するなりすましの危険性を回避し、また、生体情報を利用する場合、怪我等の使用する部位の状態、体調、更には指紋認証を例に取ると、生まれつき指紋が薄くて認証には適さない等、生まれながらの特性により完全な本人認証ができない場合に対応するＩＣカード、登録装置、及びサービス提供システムを実現できるという効果が得られる。

【図面の簡単な説明】

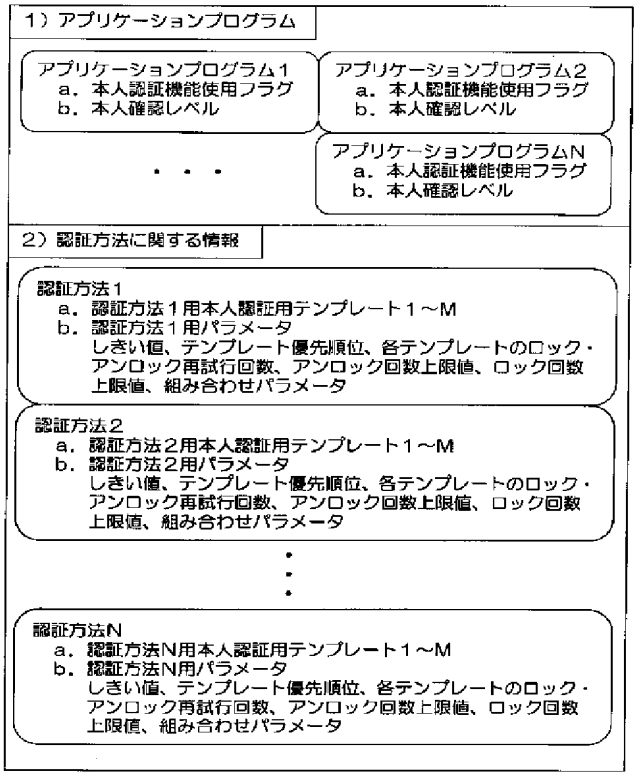
【図１】　本発明の実施の形態のＩＣカード上に構成される機能ブロックを説明するブロック図である。

【図２】　同実施の形態のＩＣカード上のＥＥＰＲＯＭに記録される情報の構成を説明する模式図である。
【図３】　同実施の形態のＩＣカード上のＥＥＰＲＯＭに記録される情報の構成を説明する模式図である。
【図４】　同実施の形態のＩＣカードへの本人認証機能の登録動作を説明するフローチャートである。
【図５】　本人認証機能の登録時のＩＣカードへの登録認証動作の一例を説明するシーケンス図である。
【図６】　同実施の形態のＩＣカードへのアプリケーションプログラムの登録・削除動作を説明するフローチャートである。
【図７】　アプリケーションの登録・削除時のアプリケーション鍵による認証動作の一例を説明するシーケンス図である。
【図８】　アプリケーションの登録・削除時のアプリケーション鍵による認証動作の一例を説明するシーケンス図である。
【図９】　同実施の形態のＩＣカードで実行されるアプリケーションが１つの認証方法を実行する場合の動作を説明するフローチャートである。
【図１０】　同実施の形態のＩＣカードで実行されるアプリケーションが複数の認証方法を優先順位により選択して実行する場合の動作を説明するフローチャートである。
【図１１】　同実施の形態のＩＣカードで実行される複数のアプリケーションが認証結果を共有する場合の動作を説明するフローチャートである。
【図１２】　同実施の形態のＩＣカードのカード所持者による本人認証機能のメンテナンス動作を説明するフローチャートである。
【図１３】　同実施の形態のＩＣカードのカード所持者による本人認証機能のメンテナンス動作を説明するフローチャートである。
【図１４】　同実施の形態のＩＣカードのシステム管理者による本人認証機能のメンテナンス動作を説明するフローチャートである。
【図１５】　本発明の実施例のシステム構成を説明するブロック図である。
【図１６】　本発明の実施例の認証データ登録ＩＣカード発行機によるＩＣカード発行動作を説明するシーケンス図である。
【図１７】　本発明の実施例のＩＣカード自販機によるＩＣカード入手動作を説明するシーケンス図である。
【図１８】　本発明の実施例のＩＣカード内アプリケーション構成例を説明する模式図である。
【図１９】　本発明の実施例のＩＣカード内のパスワードによる認証方法リストの詳細を説明する模式図である。
【図２０】　本発明の実施例のＩＣカード内の指紋照合による認証方法リストの詳細を説明する模式図である。
【図２１】　本発明の実施例のＩＣカード内の音声照合による認証方法リストの詳細を説明する模式図である。
【図２２】　本発明の実施例の病院用ＩＤカードアプリケーションの動作を説明するシーケンス図である。
【図２３】　本発明の実施例の病院用ＩＤカードアプリケーションの動作を説明するシーケンス図である。
【図２４】　ＩＣカードと病院または店舗用のアプリケーションとの相互認証動作の一例を説明するシーケンス図である。
【図２５】　ＩＣカードと病院または店舗用のアプリケーションとの相互認証動作の一例を説明するシーケンス図である。
【図２６】　本発明の実施例のキャッシュカードアプリケーションの動作を説明するシーケンス図である。
【図２７】　本発明の実施例のＩＣカード内に２つのテンプレートが存在する場合のテンプレート選択動作を説明するフローチャートである。
【符号の説明】
１　制御処理部
２　入出力制御部
３　ＥＥＰＲＯＭ
４　ＲＯＭ
５　ＲＡＭ
１１　アプリケーション追加・削除機能部
１２　データ読み・書き処理部
１３　コマンド実行管理部
１４　本人認証機能部
１０１　顧客管理サーバ
１０２　認証データ登録ＩＣカード発行機
１０３　クライアント端末
１０４　スキャナまたは照合装置
１０５　ＩＣカード自動販売機
１０６　ＩＣカード販売管理サーバ
１０７　コンピュータネットワーク

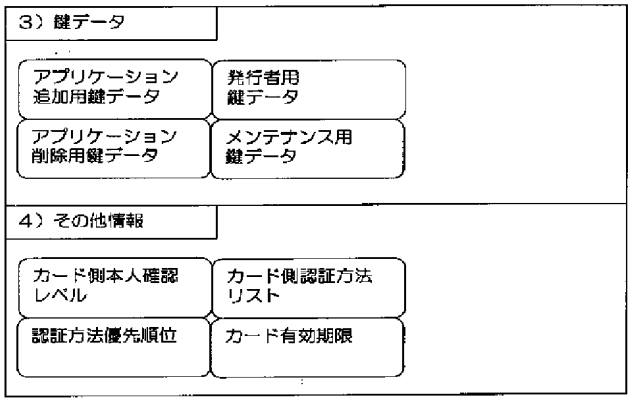
【図1】


1：制御処理部
12
データ読み・書き処理部
11
アプリケーション追加・削除機能部
14
本人認証機能部
13
コマンド実行管理部
3
EEPROM
4
ROM
5
RAM
2
入出力制御部
R／W装置へ

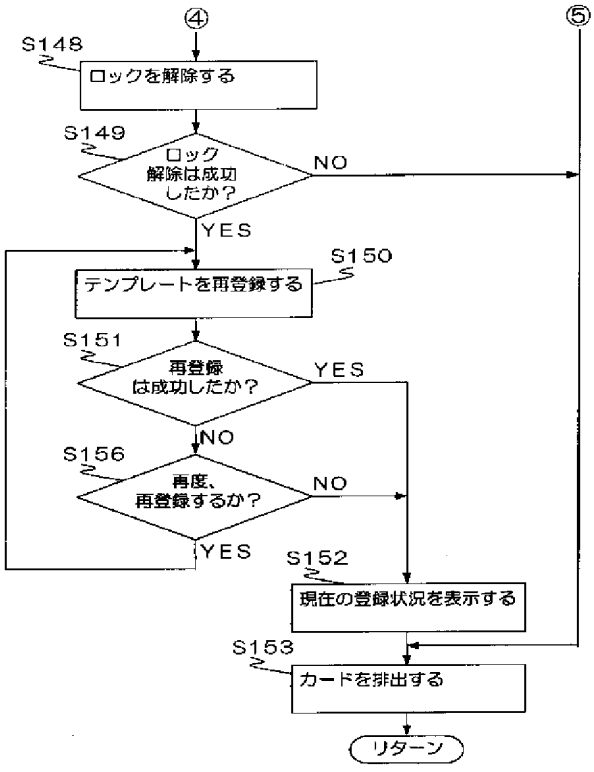
【図2】


1）アプリケーションプログラム
アプリケーションプログラム1
a．本人認証機能使用フラグ
b．本人確認レベル
アプリケーションプログラム2
a．本人認証機能使用フラグ
b．本人確認レベル
アプリケーションプログラムN
a．本人認証機能使用フラグ
b．本人確認レベル
2）認証方法に関する情報
認証方法1
a．認証方法1用本人認証用テンプレート1～M
b．認証方法1用パラメータ
しきい値、テンプレート優先順位、各テンプレートのロック・アンロック再試行回数、アンロック回数上限値、ロック回数上限値、組み合わせパラメータ
認証方法2
a．認証方法2用本人認証用テンプレート1～M
b．認証方法2用パラメータ
しきい値、テンプレート優先順位、各テンプレートのロック・アンロック再試行回数、アンロック回数上限値、ロック回数上限値、組み合わせパラメータ
認証方法N
a．認証方法N用本人認証用テンプレート1～M
b．認証方法N用パラメータ
しきい値、テンプレート優先順位、各テンプレートのロック・アンロック再試行回数、アンロック回数上限値、ロック回数上限値、組み合わせパラメータ

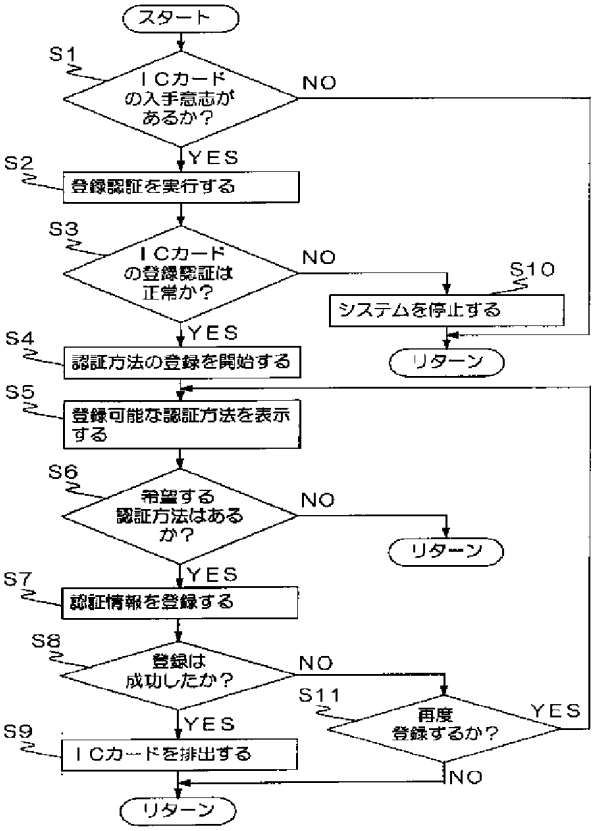
【図3】


3）鍵データ
アプリケーション追加用鍵データ
発行者用鍵データ
アプリケーション削除用鍵データ
メンテナンス用鍵データ
4）その他情報
カード側本人確認レベル
カード側認証方法リスト
認証方法優先順位
カード有効期限

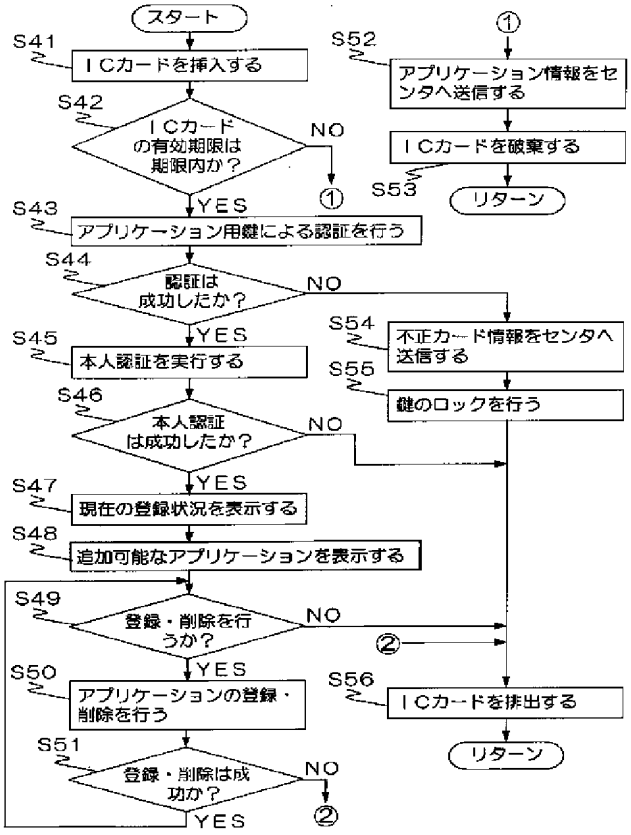
【図13】


④
⑤
S148
ロックを解除する
S149
ロック解除は成功したか？
NO
YES
S150
テンプレートを再登録する
S151
再登録は成功したか？
YES
NO
S156
再度、再登録するか？
NO
YES
S152
現在の登録状況を表示する
S153
カードを排出する
リターン

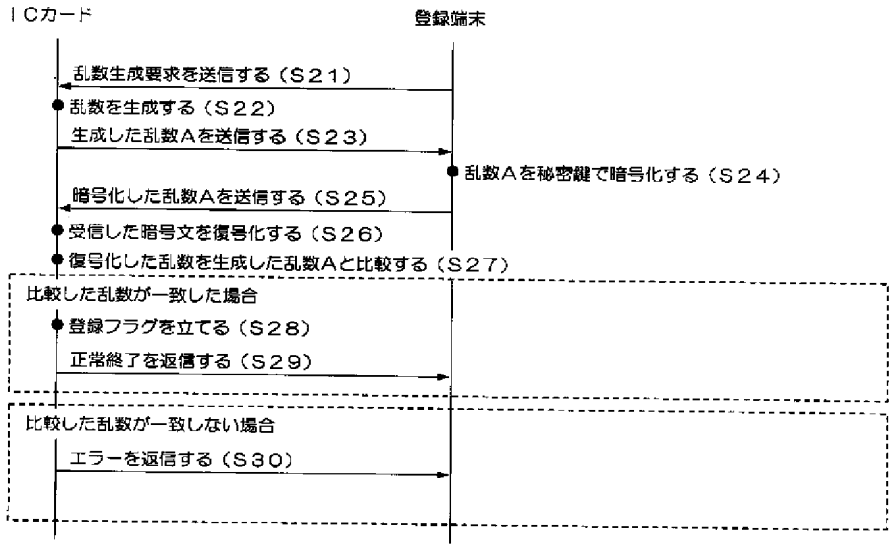
【図４】


スタート
S1
ＩＣカードの入手意志があるか？
NO
YES
S2
登録認証を実行する
S3
ＩＣカードの登録認証は正常か？
NO
S10
システムを停止する
YES
S4
認証方法の登録を開始する
リターン
S5
登録可能な認証方法を表示する
S6
希望する認証方法はあるか？
NO
リターン
YES
S7
認証情報を登録する
S8
登録は成功したか？
NO
S11
再度登録するか？
YES
YES
S9
ＩＣカードを排出する
NO
リターン

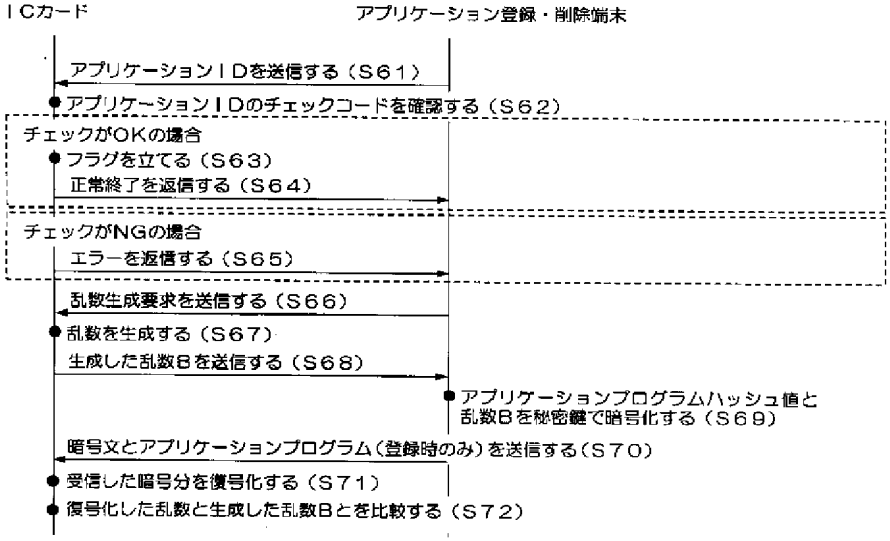
【図６】


スタート
S41
ＩＣカードを挿入する
S42
ＩＣカードの有効期限は期限内か？
NO
①
YES
S43
アプリケーション用鍵による認証を行う
S44
認証は成功したか？
NO
YES
S45
本人認証を実行する
S46
本人認証は成功したか？
NO
YES
S47
現在の登録状況を表示する
S48
追加可能なアプリケーションを表示する
S49
登録・削除を行うか？
NO
②
YES
S50
アプリケーションの登録・削除を行う
S51
登録・削除は成功か？
NO
②
YES
①
S52
アプリケーション情報をセンタへ送信する
ＩＣカードを破棄する
S53
リターン
S54
不正カード情報をセンタへ送信する
S55
鍵のロックを行う
S56
ＩＣカードを排出する
リターン

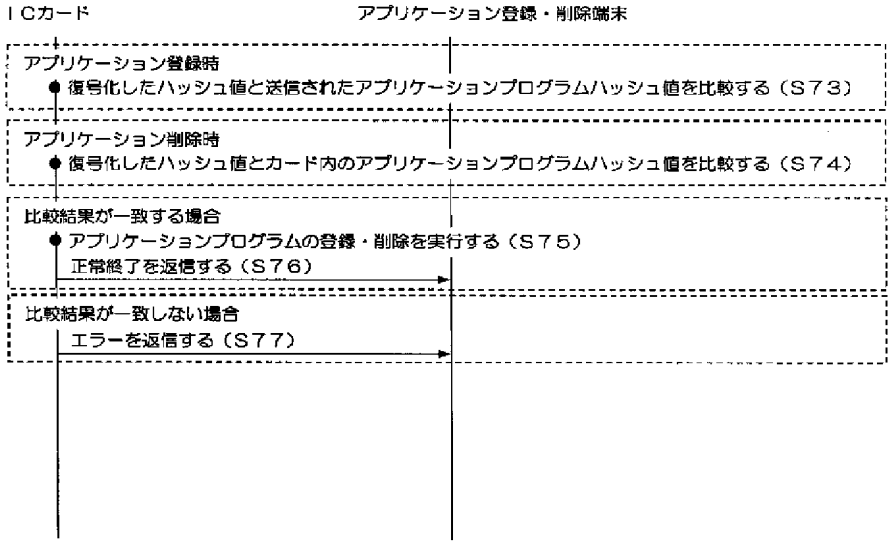
【図５】


ＩＣカード
登録端末
乱数生成要求を送信する（Ｓ２１）
乱数を生成する（Ｓ２２）
生成した乱数Ａを送信する（Ｓ２３）
乱数Ａを秘密鍵で暗号化する（Ｓ２４）
暗号化した乱数Ａを送信する（Ｓ２５）
受信した暗号文を復号化する（Ｓ２６）
復号化した乱数を生成した乱数Ａと比較する（Ｓ２７）
比較した乱数が一致した場合
登録フラグを立てる（Ｓ２８）
正常終了を返信する（Ｓ２９）
比較した乱数が一致しない場合
エラーを返信する（Ｓ３０）

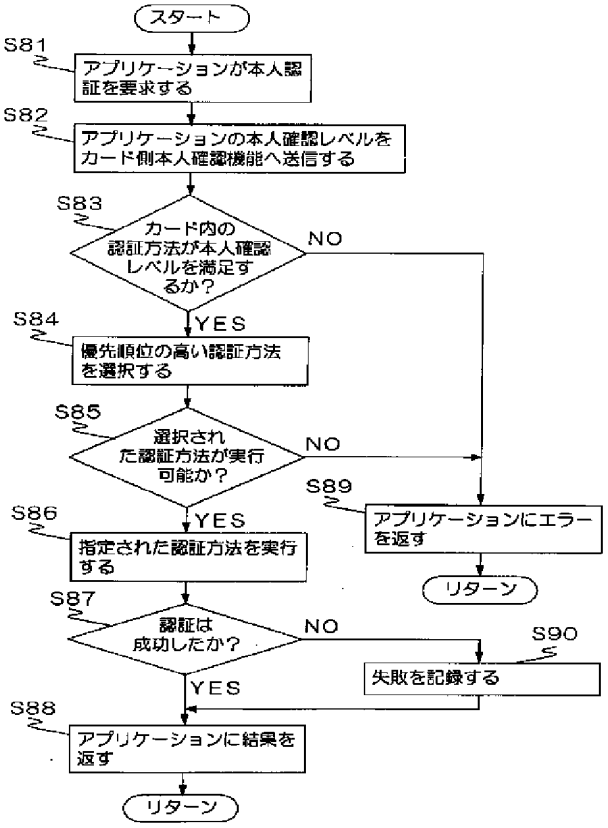
【図7】


ICカード
アプリケーション登録・削除端末
アプリケーションIDを送信する（S61）
アプリケーションIDのチェックコードを確認する（S62）
チェックがOKの場合
フラグを立てる（S63）
正常終了を返信する（S64）
チェックがNGの場合
エラーを返信する（S65）
乱数生成要求を送信する（S66）
乱数を生成する（S67）
生成した乱数Bを送信する（S68）
アプリケーションプログラムハッシュ値と
乱数Bを秘密鍵で暗号化する（S69）
暗号文とアプリケーションプログラム（登録時のみ）を送信する（S70）
受信した暗号分を復号化する（S71）
復号化した乱数と生成した乱数Bとを比較する（S72）

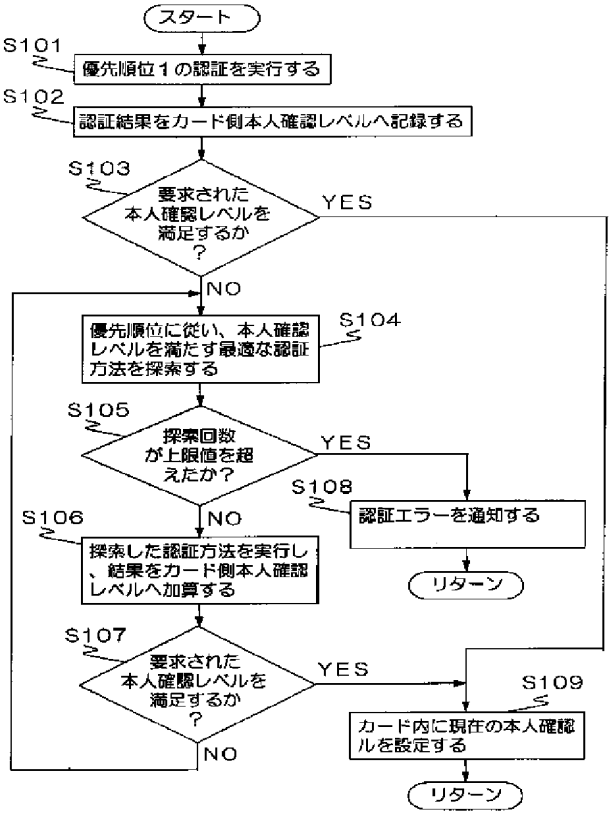
【図8】


ICカード
アプリケーション登録・削除端末
アプリケーション登録時
復号化したハッシュ値と送信されたアプリケーションプログラムハッシュ値を比較する（S73）
アプリケーション削除時
復号化したハッシュ値とカード内のアプリケーションプログラムハッシュ値を比較する（S74）
比較結果が一致する場合
アプリケーションプログラムの登録・削除を実行する（S75）
正常終了を返信する（S76）
比較結果が一致しない場合
エラーを返信する（S77）

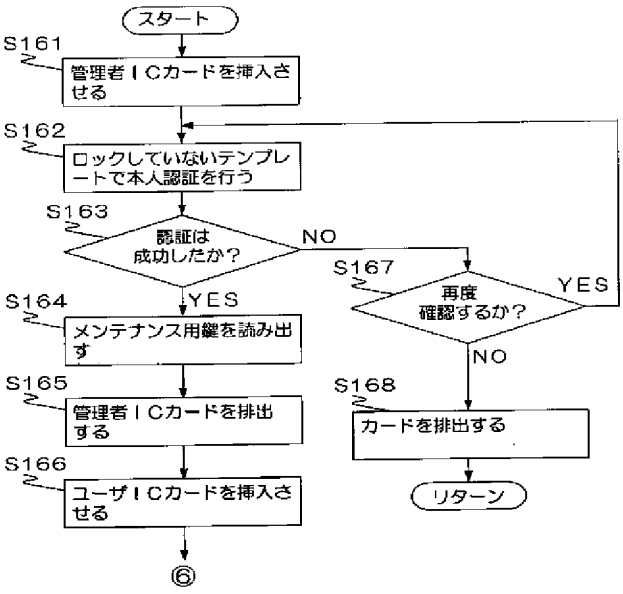
【図9】


スタート
S81
アプリケーションが本人認証を要求する
S82
アプリケーションの本人確認レベルをカード側本人確認機能へ送信する
S83
カード内の認証方法が本人確認レベルを満足するか?
NO
YES
S84
優先順位の高い認証方法を選択する
S85
選択された認証方法が実行可能か?
NO
YES
S86
指定された認証方法を実行する
S87
認証は成功したか?
NO
YES
S88
アプリケーションに結果を返す
リターン
S89
アプリケーションにエラーを返す
リターン
S90
失敗を記録する

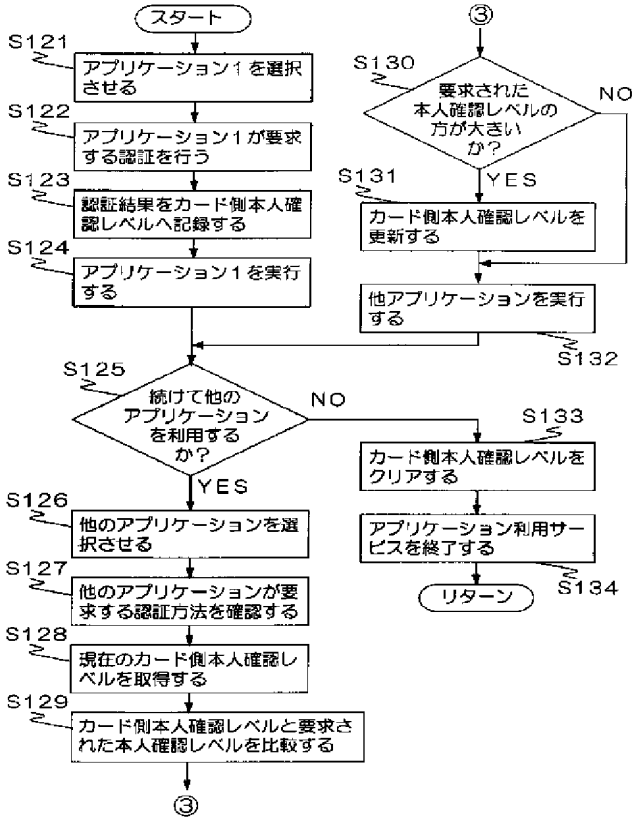
【図10】


スタート
S101
優先順位1の認証を実行する
S102
認証結果をカード側本人確認レベルへ記録する
S103
要求された本人確認レベルを満足するか?
YES
NO
S104
優先順位に従い、本人確認レベルを満たす最適な認証方法を探索する
S105
探索回数が上限値を超えたか?
YES
NO
S106
探索した認証方法を実行し、結果をカード側本人確認レベルへ加算する
S107
要求された本人確認レベルを満足するか?
YES
NO
S108
認証エラーを通知する
リターン
S109
カード内に現在の本人確認レベルを設定する
リターン

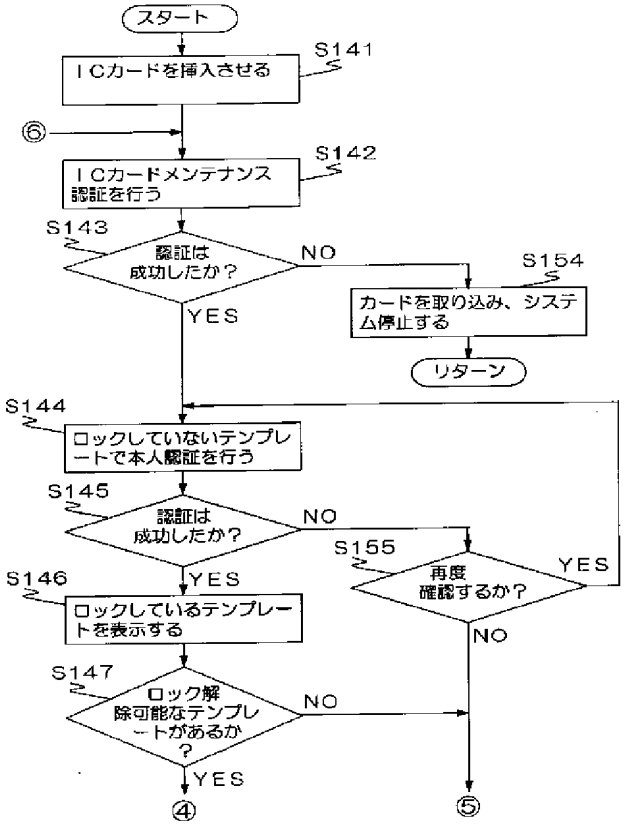
【図14】


スタート
S161
管理者ICカードを挿入させる
S162
ロックしていないテンプレートで本人認証を行う
S163
認証は成功したか?
NO
YES
S164
メンテナンス用鍵を読み出す
S165
管理者ICカードを排出する
S166
ユーザICカードを挿入させる
⑥
S167
再度確認するか?
YES
NO
S168
カードを排出する
リターン

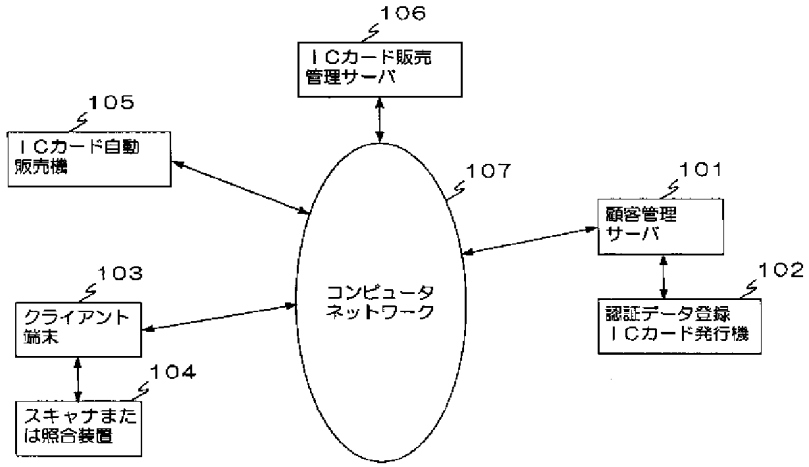
【図11】


スタート
S121
アプリケーション1を選択させる
S122
アプリケーション1が要求する認証を行う
S123
認証結果をカード側本人確認レベルへ記録する
S124
アプリケーション1を実行する
S125
続けて他のアプリケーションを利用するか？
NO
YES
S126
他のアプリケーションを選択させる
S127
他のアプリケーションが要求する認証方法を確認する
S128
現在のカード側本人確認レベルを取得する
S129
カード側本人確認レベルと要求された本人確認レベルを比較する
③
③
S130
要求された本人確認レベルの方が大きいか？
NO
YES
S131
カード側本人確認レベルを更新する
他アプリケーションを実行する
S132
S133
カード側本人確認レベルをクリアする
アプリケーション利用サービスを終了する
S134
リターン

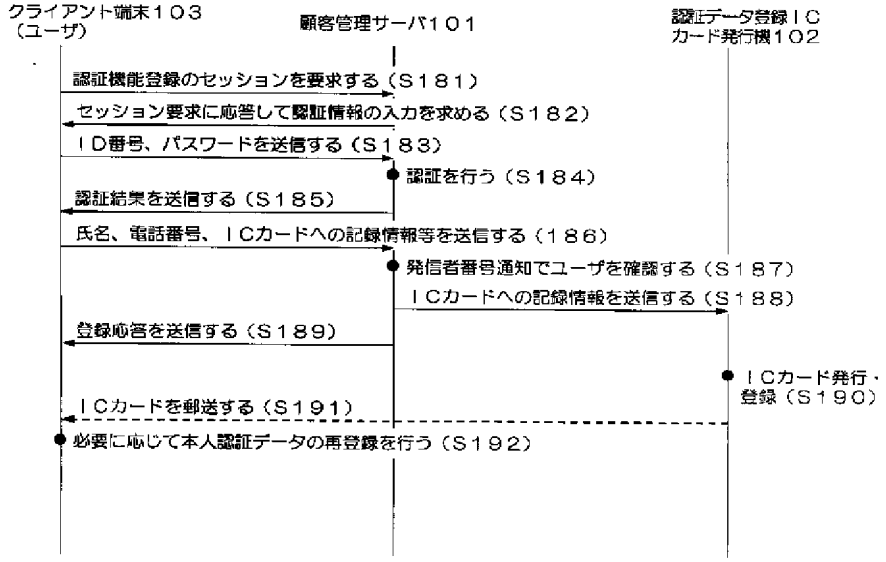
【図12】


スタート
S141
ICカードを挿入させる
⑥
S142
ICカードメンテナンス認証を行う
S143
認証は成功したか？
NO
YES
S154
カードを取り込み、システム停止する
リターン
S144
ロックしていないテンプレートで本人認証を行う
S145
認証は成功したか？
NO
YES
S155
再度確認するか？
YES
NO
S146
ロックしているテンプレートを表示する
S147
ロック解除可能なテンプレートがあるか？
NO
YES
④
⑤

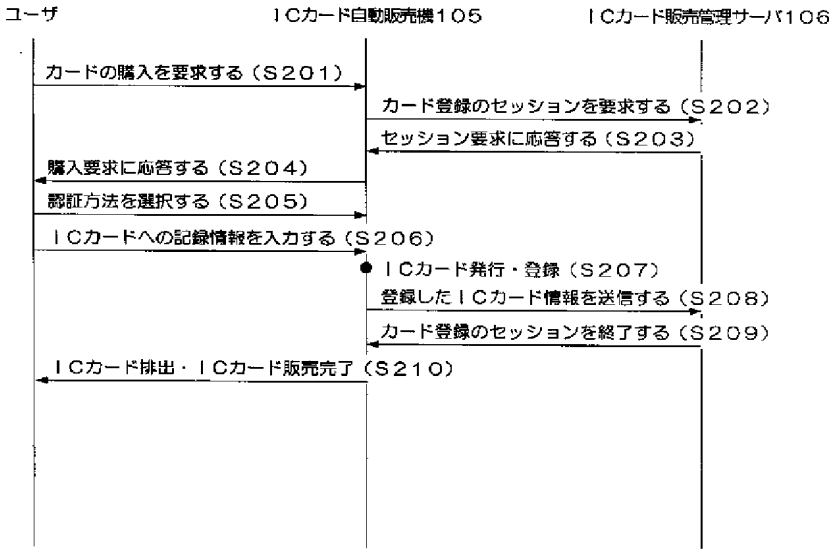
【図15】


106
ICカード販売管理サーバ
105
ICカード自動販売機
107
101
顧客管理サーバ
103
クライアント端末
コンピュータネットワーク
102
認証データ登録ICカード発行機
104
スキャナまたは照合装置

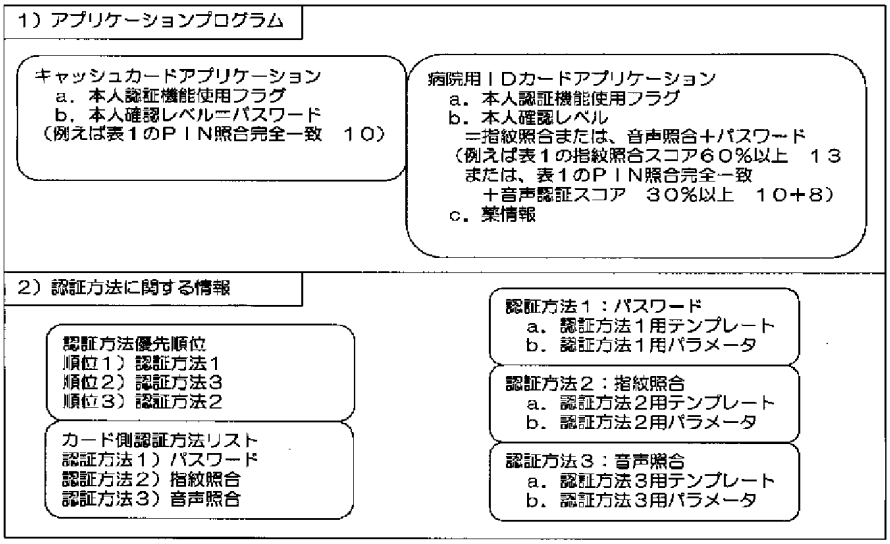
【図16】


クライアント端末103
（ユーザ）
顧客管理サーバ101
認証データ登録ICカード発行機102
認証機能登録のセッションを要求する（S181）
セッション要求に応答して認証情報の入力を求める（S182）
ID番号、パスワードを送信する（S183）
認証を行う（S184）
認証結果を送信する（S185）
氏名、電話番号、ICカードへの記録情報等を送信する（186）
発信者番号通知でユーザを確認する（S187）
ICカードへの記録情報を送信する（S188）
登録応答を送信する（S189）
ICカード発行・登録（S190）
ICカードを郵送する（S191）
必要に応じて本人認証データの再登録を行う（S192）

【図17】


ユーザ
ICカード自動販売機105
ICカード販売管理サーバ106
カードの購入を要求する（S201）
カード登録のセッションを要求する（S202）
セッション要求に応答する（S203）
購入要求に応答する（S204）
認証方法を選択する（S205）
ICカードへの記録情報を入力する（S206）
ICカード発行・登録（S207）
登録したICカード情報を送信する（S208）
カード登録のセッションを終了する（S209）
ICカード排出・ICカード販売完了（S210）

【図１８】



【図１９】

認証方法１：パスワード

a．認証方法１用テンプレート

テンプレート　：　１２３４

テンプレート　：　２３４５

b．認証方法１用パラメータ

しきい値	１００％
テンプレート優先順位	なし
ロック再試行回数	テンプレート１＝５回 テンプレート２＝３回
アンロック再試行回数	テンプレート１＝３回 テンプレート２＝２回
アンロック回数上限値	３回
ロック回数上限値	５回
組み合わせパラメータ	テンプレート１とテンプレート２を同時に照合し、失敗したら両方のテンプレートの再試行回数を減らす。

【図２０】

認証方法２：指紋照合
ａ．認証方法２用テンプレート
左手人差し指テンプレート　：＊＊＊＊＊＊＊＊＊＊…＊＊
右手人差し指テンプレート　：＊＊＊＊…＊＊

ｂ．認証方法２用パラメータ

しきい値	７５％
テンプレート優先順位	２
ロック再試行回数	テンプレート１＝１０回 テンプレート２＝９回
アンロック再試行回数	テンプレート１＝３回 テンプレート２＝２回
アンロック回数上限値	３回
ロック回数上限値	１０回
組み合わせパラメータ	優先順位の早い順に、一指づつ照合する。 一指に３回失敗したら、次の指の照合に入る。 次の指の照合を行うかは、外部からの信号による。

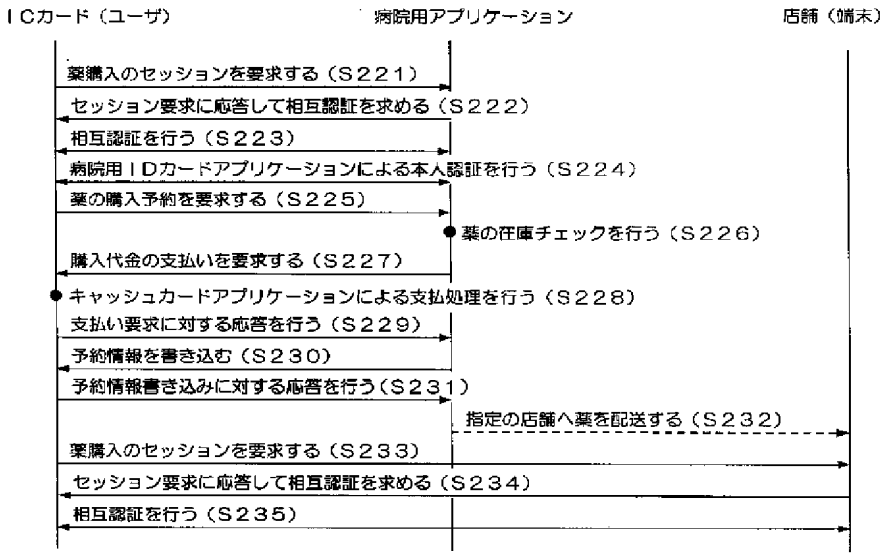
【図２１】

認証方法３：音声照合
ａ．認証方法３用テンプレート
音声テンプレート　：＊＊＊＊＊＊＊＊＊＊…＊＊
音声テンプレート　：＊＊＊＊…＊＊

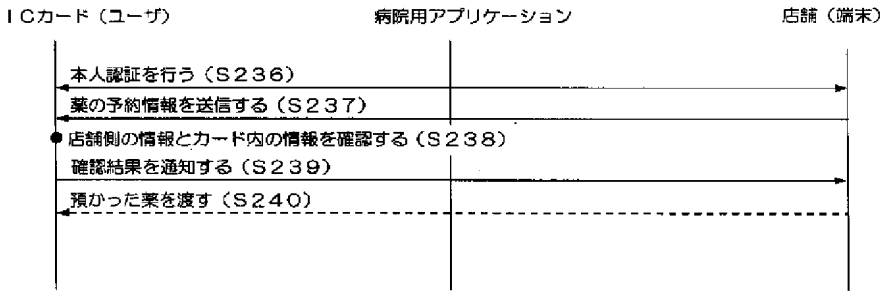
ｂ．認証方法３用パラメータ

しきい値	４０％
テンプレート優先順位	１
ロック再試行回数	テンプレート１＝１５回 テンプレート２＝１４回
アンロック再試行回数	テンプレート１＝５回 テンプレート２＝５回
アンロック回数上限値	５回
ロック回数上限値	１５回
組み合わせパラメータ	両方の音声テンプレートを続けて照合し、 両方の類似度の平均がしきい値以上であること を確認する。

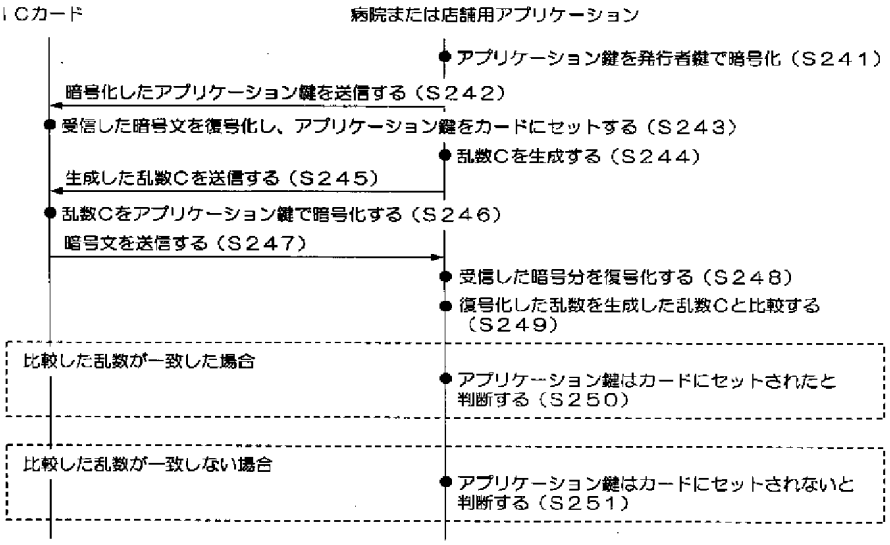
【図２２】


ＩＣカード（ユーザ）
病院用アプリケーション
店舗（端末）
薬購入のセッションを要求する（Ｓ２２１）
セッション要求に応答して相互認証を求める（Ｓ２２２）
相互認証を行う（Ｓ２２３）
病院用ＩＤカードアプリケーションによる本人認証を行う（Ｓ２２４）
薬の購入予約を要求する（Ｓ２２５）
薬の在庫チェックを行う（Ｓ２２６）
購入代金の支払いを要求する（Ｓ２２７）
キャッシュカードアプリケーションによる支払処理を行う（Ｓ２２８）
支払い要求に対する応答を行う（Ｓ２２９）
予約情報を書き込む（Ｓ２３０）
予約情報書き込みに対する応答を行う（Ｓ２３１）
指定の店舗へ薬を配送する（Ｓ２３２）
薬購入のセッションを要求する（Ｓ２３３）
セッション要求に応答して相互認証を求める（Ｓ２３４）
相互認証を行う（Ｓ２３５）

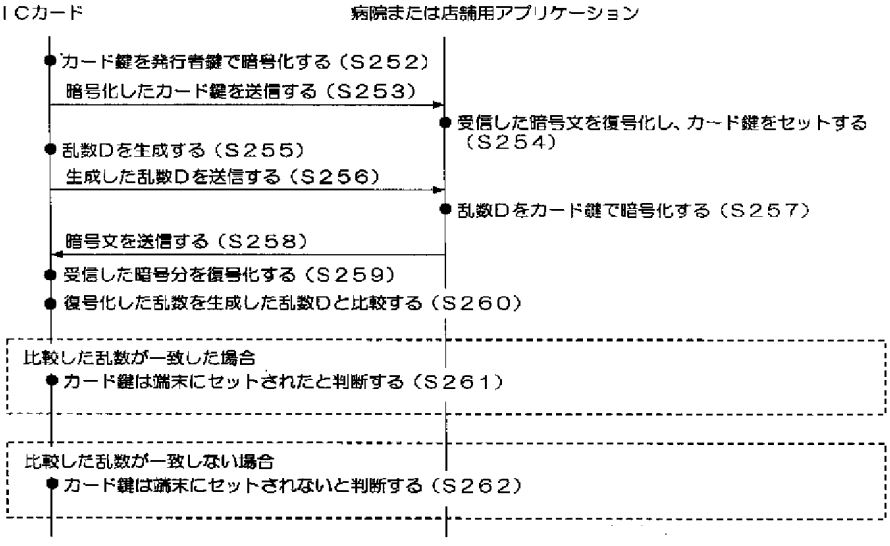
【図２３】


ＩＣカード（ユーザ）
病院用アプリケーション
店舗（端末）
本人認証を行う（Ｓ２３６）
薬の予約情報を送信する（Ｓ２３７）
店舗側の情報とカード内の情報を確認する（Ｓ２３８）
確認結果を通知する（Ｓ２３９）
預かった薬を渡す（Ｓ２４０）

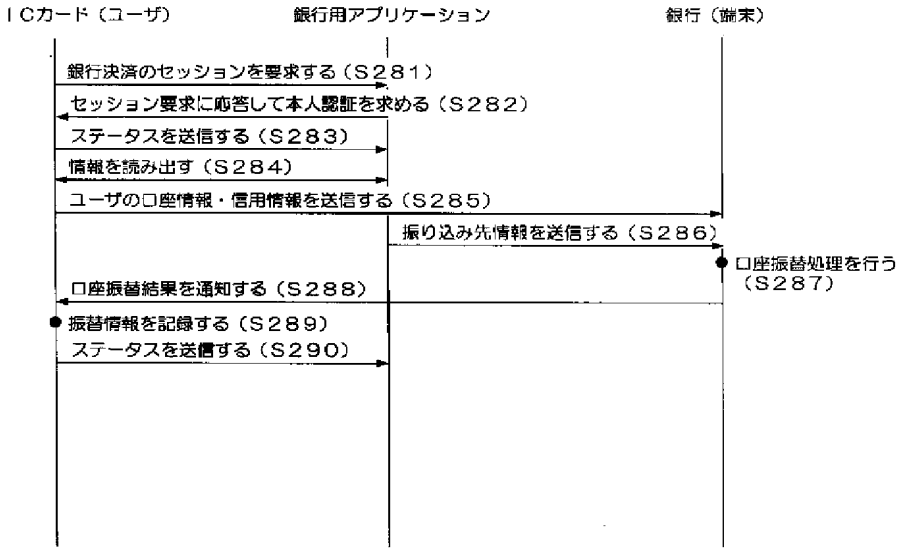
【図24】


ICカード
病院または店舗用アプリケーション
アプリケーション鍵を発行者鍵で暗号化（S241）
暗号化したアプリケーション鍵を送信する（S242）
受信した暗号文を復号化し、アプリケーション鍵をカードにセットする（S243）
乱数Cを生成する（S244）
生成した乱数Cを送信する（S245）
乱数Cをアプリケーション鍵で暗号化する（S246）
暗号文を送信する（S247）
受信した暗号分を復号化する（S248）
復号化した乱数を生成した乱数Cと比較する（S249）
比較した乱数が一致した場合
アプリケーション鍵はカードにセットされたと判断する（S250）
比較した乱数が一致しない場合
アプリケーション鍵はカードにセットされないと判断する（S251）

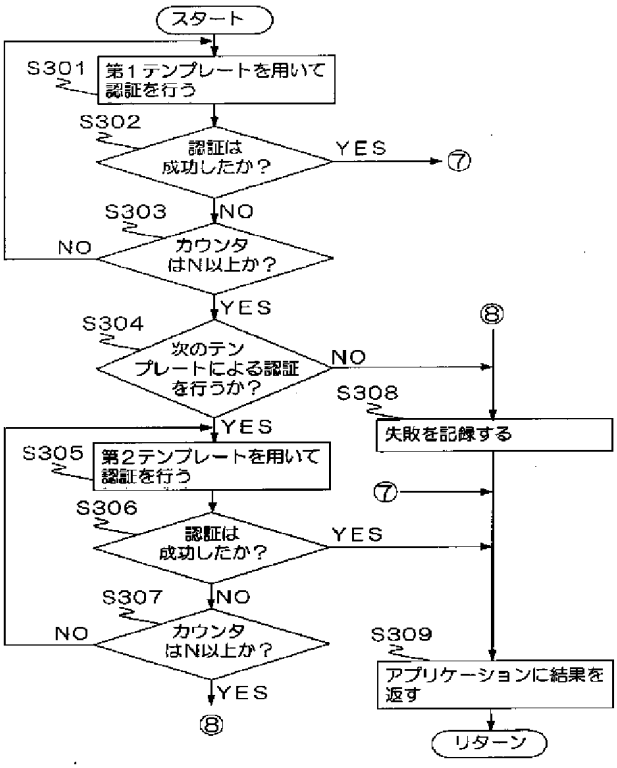
【図25】


ICカード
病院または店舗用アプリケーション
カード鍵を発行者鍵で暗号化する（S252）
暗号化したカード鍵を送信する（S253）
受信した暗号文を復号化し、カード鍵をセットする（S254）
乱数Dを生成する（S255）
生成した乱数Dを送信する（S256）
乱数Dをカード鍵で暗号化する（S257）
暗号文を送信する（S258）
受信した暗号分を復号化する（S259）
復号化した乱数を生成した乱数Dと比較する（S260）
比較した乱数が一致した場合
カード鍵は端末にセットされたと判断する（S261）
比較した乱数が一致しない場合
カード鍵は端末にセットされないと判断する（S262）

【図26】


ICカード（ユーザ）
銀行用アプリケーション
銀行（端末）
銀行決済のセッションを要求する（S281）
セッション要求に応答して本人認証を求める（S282）
ステータスを送信する（S283）
情報を読み出す（S284）
ユーザの口座情報・信用情報を送信する（S285）
振り込み先情報を送信する（S286）
口座振替処理を行う（S287）
口座振替結果を通知する（S288）
振替情報を記録する（S289）
ステータスを送信する（S290）

【図27】


スタート
S301
第1テンプレートを用いて認証を行う
S302
認証は成功したか？
YES
⑦
NO
S303
カウンタはN以上か？
NO
YES
S304
次のテンプレートによる認証を行うか？
NO
⑧
S308
失敗を記録する
YES
S305
第2テンプレートを用いて認証を行う
⑦
S306
認証は成功したか？
YES
S307
NO
カウンタはN以上か？
NO
YES
⑧
S309
アプリケーションに結果を返す
リターン

フロントページの続き

Ｆターム(参考)　2C005 MA04 SA11
5B035 AA14 BB09 BC01 CA38
5B055 BB10 EE03 HA01 HA14 KK05
KK13 KK14
5B076 FB05
5B085 AE12